TAMPEREEN YLIOPISTO
Johtamiskorkeakoulu

KYBERRISKEILTÄ SUOJAUTUMINEN JA KYBERVAKUUTUSMARKKINAT SUOMESSA

Vakuutustiede
Pro gradu-tutkielma
Huhtikuu 2017
Tekijä: Tia-Liisa Roikola

Ohjaaja: Lasse Koskinen

TIIVISTELMÄ

Tampereen yliopisto	Johtamiskorkeakoulu: vakuutustiede
Tekijä:	ROIKOLA, TIA-LIISA
Tutkielman nimi:	Kyberriskeiltä suojautuminen ja kybervakuutusmarkkinat Suomessa
Pro gradu – tutkielma:	74 sivua, 2 liitesivua
Aika:	Huhtikuu 2017
Avainsanat:	Kyberriskit, kybervakuutus, kybervakuutusmarkkinat, riskienhallinta

---

Teknologia ja digitalisoituminen ovat mahdollistaneet paljon, mutta samalla altistaneet maailman uudenlaisille riskeille. Kyberriskit ovat esimerkki näistä uusista riskeistä, jotka ovat lisääntyneet merkittävästi viimeisen kymmenen vuoden aikana, koska yhä useammat laitteet on yhdistetty internettiin. Kyberriskit ovat tänä päivänä laajalle levinneitä ja yritykset niiden koosta ja toimialasta riippumatta altistuvat näille riskeille.

Tämän tutkimuksen tarkoituksena oli selvittää miten suomalaiset yritykset ovat suojautuneet kyberriskeiltä sekä millaiset ovat Suomen kybervakuutusmarkkinat vuonna 2016. Kyberilmiö on Suomessa vielä toistaiseksi vähän tutkittu aihe ja samalla äärimmäisen ajankohtainen. Myös vakuutusyhtiöt ovat reagoineet tähän uuteen riskiin lanseeraamalla kybervakuutuksen. Ensimmäiset kybervakuutus tuotteet lanseerattiin jo kymmenisen vuotta sitten Yhdysvalloissa. Suomessa kybervakuutusta alettiin myydä noin neljä vuotta sitten ulkomaalaisen vakuutusyhtiön toimesta ja viimeisen vuoden aikana myös osa suomalaisista vakuutusyhtiöistä on ottanut kybervakuutuksen tuotevalikoimaansa, vastatakseen tähän jatkuvasti kasvavaan riskiin.

Tutkimus toteutettiin käyttäen kvalitatiivista tutkimusmenetelmää ja tutkimusmetodina toimivat teemahaastattelut. Tutkimuksessa haastateltiin kuutta eri kyberriski ja kybervakuutus asiantuntijaa, jotka muodostivat tutkimuksen empiirisen osion. Tutkimuksessa syvennyttiin ensin kyberriskeiltä suojautumisen keinoihin, jonka jälkeen tutkittiin kybervakuutusmarkkinoiden tilaa Suomessa vuonna 2016. Yhteenvetona tutkimustuloksista voidaan todeta, että Suomessa kyberriskitietoisuus on jatkuvasti nousussa kaiken kokoisissa yhtiöissä. Riskitietoisuuden ja riskeiltä suojautumisen taso vaihtelee yrityskoon mukaan. Suomen kybervakuutusmarkkinoilla on kova kilpailu ja kybervakuutuksen hinnat ovat alhaiset pienestä vahinkokehityksestä johtuen. Tästä huolimatta kybervakuutuksen myynti koetaan haastavaksi. Merkittävä tutkimustulos oli myös se, että yrityksillä ja vakuutusyhtiöillä on hyvin erilainen näkemys kybervakuutuksen tarpeellisuudesta.

Tutkimuksen perusteella voidaan sanoa, että kybervakuutus ei ole vielä täysin ottanut paikkaansa Suomen vakuutusmarkkinoilla, mutta tulevaisuus näyttää kuitenkin lupaavalta yritysten kasvavan riskitietoisuuden, riskien lisääntymisen sekä muun muassa uudistuvan EU:n tietosuojalainsäädännön johdosta.

SISÄLLYSLUETTELO

1 JOHDANTO

1.1 Tutkielman taustaa

Teknologia ja sen lisääntyminen ja globalisoituminen on tuonut maailmaan uudenlaisia riskejä viimeisen 20 vuoden aikana. Digitalisoituminen on tuonut ihmiskunnalle suuria etuja, mutta muodostanut samalla myös merkittäviä riskejä, joille altistumme. (Irm 2014, 7) Kyberriskit ovat yksi esimerkki näistä uudenlaisista riskeistä, joita teknologia ja digitalisoituminen on tuonut. Kyberriskeillä tarkoitetaan riskejä, jotka liittyvät informaatio teknologiaan, virtuaalitodellisuuteen sekä tietokoneiden käyttöön. Kyberriskejä ovat muun muassa tietomurrot, palvelunestohyökkäykset, internet-yhteyden kaatuminen ja yrityksen tai yksilön tietoverkkojen sabotointi. (Willis 2013) Kyberriskit ovat uhka niin yrityksille kuin yksilöillekin ja yritykset ovat alttiita kyberriskeille, jos ne tukeutuvat teknologiaan jollain tasolla. Kyberriskit eivät ole enää huoli, joka koskee ainoastaan turvallisuus ja teknologia yrityksiä vaan riski on todellinen kaiken kokoisille yrityksille toimialasta riippumatta. Vuoden 2014 aikana jokainen toimiala maailmanlaajuisesti kärsi jonkin asteisesta kyberrikoksesta ja ne ovatkin jatkuvasti kasvava ja laajeneva trendi. (PwC 2014,4)

Yhä useampi yritys siirtyy internettiin ja yhtiöiden, joiden liiketoiminta perustuu pelkästään internetin kautta tapahtuvaan kaupankäyntiin, on täysin riippuvainen tietoverkoista ja niiden toimimisesta. Esimerkiksi Amazon.com toimii ainoastaan tietoverkossa ja jos hakkeri onnistuisi vahingoittamaan sen operaatioita, menettäisi yhtiö liikevaihtonsa koko siltä ajalta, kunnes tietojärjestelmät on korjattu. (Mukhopadhyay, Saha, Chakrabarti, Mahanti & Podder 2005, 154) Yrityksen tietoverkoissa tapahtuvien häiriöiden myötä yritykselle voi siis aiheutua rahallisia tappioita yritystoiminnan tilapäisestä keskeytymisestä. Yrityksen asiakaskunnan tietojen menettämisestä ja niiden päätymisestä vääriin käsiin voi myös seurata maineen sekä asiakkaiden menetys sen lisäksi, että jo pelkästään asiakkaille tapahtuneesta tiedottamisesta aiheutuu yritykselle kustannuksia. Suomessa kyberriskeihin varautuminen ja niiden tiedostaminen on ta-

pahtunut selkeästi esimerkiksi Yhdysvaltoja myöhemmin. Limnellin (2014) mukaan kyber-käsitteen hallinnollisen institutionalisoitumisen sekä läpimurron Suomeen voidaan katsoa tapahtuneen Suomen Kyberturvallisuusstrategian myötä, joka ilmestyi vuoden 2013 alussa.

Yhdysvalloissa raportoitiin yli biljoonasta tietomurrosta viimeisen vuosikymmenen aikana. Tietomurtojen odotetaan lisääntyvän seuraavan vuosikymmenen aikana triljoonaan. Keskimääräinen tappio, joka aiheutui tietomurrosta, oli 2012 vuonna 1,2 miljoonaa dollaria. Tietomurrot aiheuttavat suuria riskejä myös muille, kun kaupallisen alan yrityksille. Esimerkiksi sairaalat altistuvat merkittävästi tälle riskille muun muassa tietokoneohjattujen implanttien takia. (Zelle & Whitehead 2014, 146) Sairaaloille voi myös syntyä merkittäviä riskejä ja kuluja, jos hakkeri pääsee käsiksi esimerkiksi sydämentahdistimiin. Sairaala voi näin joutua hakkerien kiristysuhkan alle ja kun kyse on ihmishengistä, voi kiristyssumma kasvaa merkittäväksi.

Internet of things eli asioiden internet on tuonut markkinoille useita laitteita, jotka on kytketty tietoverkkoon. Esimerkiksi kodinkoneita voi hallita tietoverkon välityksellä ja laitteet voivat myös viestiä keskenään sekä kuluttajan kanssa. Tämä tuo mahdollisuuden myös kerätä kuluttajista yhä syvällisempää tietoa ja asiakkaisiin kohdistuvan tiedon lisääntyessä on yritys myös alttiimpi tietomurroille. Yritykset käyttävät IoT laitteita kustannussäästöjen tavoitteluun sekä riskienhallintaan. IoT tarjoaa keinoja muun muassa inhimillisistä virheistä aiheutuvien kustannusten hallitsemiseen. Riskienhallinnassa se taas auttaa parantamaan omaisuuden valvontaa niin virtuaalisessa kuin fyysisessäkin maailmassa. Tietoverkkoon liitetyt laitteet tuovat kuitenkin itsessään tietoturvauhkia, joten riskienhallinnallisesti IoT:ia voidaan pitää kaksiteräisenä miekkana. (Suortti, Salmijärvi & Kupiainen 2015, 28) IoT tuo kuluttajalle etuja, mutta myös haittoja. Esimerkiksi älyautojen lisääntymisen myötä myös niiden hakkeroiminen eli autoon murtautuminen tai muuten sen tietokoneen ohjelmiston manipulointi tulee todennäköisesti yleistymään.

Koska kyberriskit ovat jatkuvasti lisääntymässä, on kehitelty myös keinoja niiltä suojautumiseksi. Ensinäkin tietokoneiden ja – järjestelmien tietoturva on oltava riittävällä tasolla. Aina se ei kuitenkaan estä hakkereita murtautumasta tietojärjestelmiin. Samalla tavalla kuin monet muutkin riskit, ovat myös kyberriskit vakuutettavissa. Kybervakuutus onkin suunniteltu yrityksille hakkereiden hyökkäyksistä aiheutuvien kustannusten pienentämiseksi ja näin liiketoiminnan jatkumisen turvaamiseksi. Esimerkiksi keskeytysvakuutus ei kata hakkerin aiheuttamasta tuotannon keskeytyksestä aiheutuvia kuluja. Yhdysvalloissa kybervakuutus kehitettiin jo

vuonna 2003 ja otettiin osaksi kyberriskijohtamista ja riskienhallintaa. (Lawrence, Loeb ja Tashfeen 2003, 81) Beazlay BNC alkoi tarjota kybervakuutusta vuonna 2010 ja vuonna 2014 sillä oli jo tuhansia asiakkaita, jotka maksavat yli 100 miljoonaa dollaria vakuutusmaksuja vuodessa. Yhdysvaltojen vakuutusmarkkinat ovat hyvin vastanneet yhtiöiden tarpeisiin suojautua kyberriskeiltä. (Zelle & Whitehead 2014, 146–147)

Kansainvälinen vakuutusyhtiö Aon alkoi 3-4 vuotta sitten tarjota kybervakuutusta Suomessa. OP-Pohjola Vakuutus toi markkinoille kybervakuutuksen 2015 syksyllä. Vakuutus on tarkoitettu suuryrityksille ja se kattaa kyberturvallisuuden vaarantumisesta aiheutuneita kuluja. (www.op.fi) Myös If on ottanut valikoimaansa tietoturvavakuutuksen. LähiTapiola on lanseeraamassa kybervakuutusta vuonna 2017. Kybervakuutuksen avulla suojaudutaan paremmin liiketoiminta- sekä maineriskeiltä ja vakuutetaan arvokasta tietopääomaa.

Kybervakuutusmarkkinoiden odotetaan kasvavan 2,5 biljoonasta dollarista 7,5 biljoonaa dollariin vuoteen 2020 mennessä. (www.forbes.com)Tulevaisuudessa kybervakuuttaminen tulee varmasti yleistymään yhä enemmän Euroopan unionin tietosuojalainsäädännön uudistuksen myötä. Keskeisenä tavoitteena on yksilön oikeuksien ja sisämarkkinaulottuvuuden lujittaminen, tietosuojan globaalin ulottuvuuden huomioon ottaminen sekä rikosasioissa tehtävää poliisi- ja oikeudellista yhteistyötä koskevien tietosuojasääntöjen tarkistaminen. Uudistuksen tavoitteena on luoda Euroopan unionille yhtenäinen, vahva ja ajanmukainen tietosuojakehys. Tarkoituksena on myös edistää EU:n digitaalisten sisämarkkinoiden kehitystä ja parantaa luottamusta online-palveluihin. Teknologian nopea kasvu ja globalisoituminen ovat tuoneet uusia haasteita henkilötietojen suojeluun. (www.oikeusministeriö.fi)Asetuksen myötä organisaatioiden on huolehdittava asiakasrekistereistään ja henkilötietokannoista yhä tarkemmin. Organisaatioilla on myös ilmoitusvelvollisuus vähäistä suurempien tietoturvaloukkausten ilmetessä. Valvontaviranomaisella on myös oikeus langettaa hallinnollisia seuraamuksia asetuksessa luetelluista teoista. (www.tietosuoja.fi)

1.2 Tutkimusongelmat ja rajaukset

Tutkimuksen tavoitteena on selvittää millä keinoin yritykset ovat varautuneet kyberriskeihin sekä kartoittaa kyberriskien ja kybervakuuttamisen tilaa 2016 luvun Suomessa. Tutkimus on rajattu koskemaan kyberriskeiltä suojautumista kybervakuutuksella ja pääpaino tutkimuksessa

pidetään tässä. Näin ollen tutkimuksessa ei niinkään paneuduta kyberriskien luonteeseen yhteiskunnassa eikä kybersodankäyntiin. Tutkimus keskittyy yrityksiin kohdistuviin kyberriskeihin ja näin yksilöön kohdistuvat kyberriskit ovat jätetty tutkimuksen ulkopuolelle. Tämä rajaus on tehty sen perusteella, että saadaan syvällisempi kuva juuri yrityksiä uhkaavista kyberriskeistä. Tutkimuksessa on tarkoitus luoda yleiskatsaus Suomen kyberriski sekä kybervakuutus kenttään ja näin ollen selventää tätä vähän tutkittua trendinomaista liiketoiminnan ja riskien osa-aluetta. Tutkimuksessa pyritään löytämään vastaukset kahteen päätutkimusongelmaan.

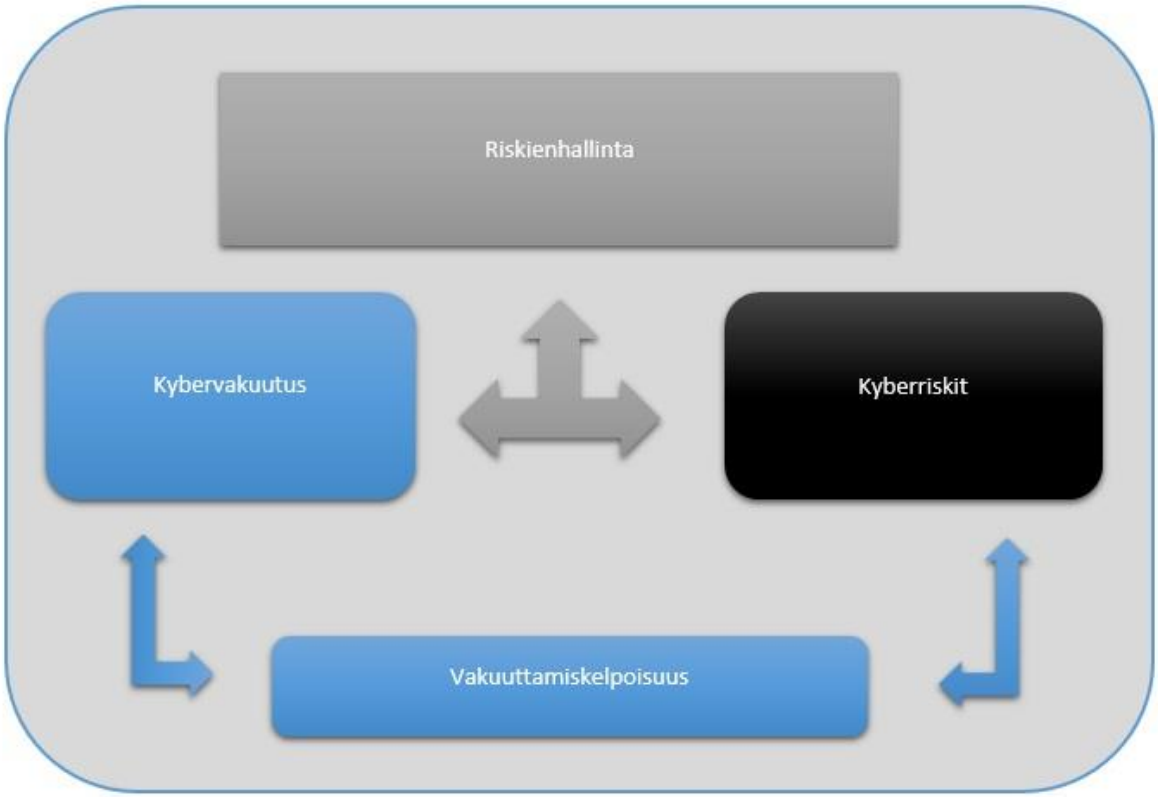
1) Miten suomalaiset yritykset ovat varautuneet kyberriskeihin?

2) Millaiset ovat Suomen kybervakuutusmarkkinat vuonna 2016?

Ensimmäiseen tutkimusongelmaan etsitään vastausta haastattelemalla kahta suomalaista erikokoista ja eri toimialalla toimivaa yhtiötä. Yrityksen valinnassa on painotettu yrityksiä, joiden liiketoiminta altistuu suuriltaosin kyberriskeille ja jotka panostavat niiltä suojautumiseen ja näin ollen tältä pohjalta voidaan tehdä yleistys kyberriskeihin varautumisesta Suomessa. Haastatteluiden avulla selvitetään yrityksen kyberriskeihin varautumisen muotoja sekä organisaation yleistä kyberriskikäsitystä eli millaisina riskeinä kyseinen organisaatio ymmärtää kyberriskit. Kyberriskeihin varautumisessa keskitytään varsinkin kybervakuutukseen ja siihen, onko yritys ottanut vai ei kybervakuutusta ja mitkä ovat syyt siihen. Tarkoituksena on kartoittaa kyberriskien asemaa organisaatioiden riskienhallinnassa sekä millaisessa asemassa riskejä pidetään muihin riskeihin nähden.

Toiseen tutkimusongelmaan etsitään vastausta vakuutusyhtiöiden asiantuntijahaastatteluiden sekä muun aineiston perusteella. Tässä tutkimusongelmassa pyritään kartoittamaan millaiset ovat Suomen kybervakuutusmarkkinat eli mikä on kybervakuuttamisen tila Suomessa vuonna 2016. Tilalla tarkoitetaan tässä tutkimuksessa kybervakuutusmarkkinoiden kokoa sekä kehittyneisyyttä, kilpailua markkinoilla sekä tuotteen tunnettuutta ja sen ominaisuuksia. Markkinoiden tilan tarkastelussa otetaan huomioon myös jälleenvakuuttajien rooli kybervakuutuksessa sekä haitallinen valikoituminen ja moraalikato. Tarkoituksena on saada kokonaiskuva Suomen kybervakuutusmarkkinoista ja miten kybervakuutus on tuotteena otettu vastaan yrityksien keskuudessa. Lisäksi perehdytään myös eri vakuutusyhtiöiden asemointiin kybervakuutusmarkkinoilla.

1.3 Tutkimuksen teoreettinen viitekehys



Kuvio 1. Teoreettinen viitekehys. Teoreettisen viitekehyksen muodostaa riskienhallinnan, kyberriskien, kybervakuutuksen sekä vakuuttamiskelpoisuuden käsitteet.

Tämän tutkimuksen teoreettisen pohjan muodostavat riskienhallinnan, kyberriskien, kybervakuutuksen sekä vakuuttamiskelpoisuuden käsitteet. Teoreettisen viitekehyksen perustana toimii riskienhallinta. Riskienhallintaa voidaan toteuttaa vakuutuksen keinoin, kun vakuutuksen avulla voidaan siirtää riskejä vakuutusyhtiölle. Jotta vakuutuksen keinoin voidaan suojautua riskiltä, on riskin oltava vakuuttamiskelpoinen. Kaikki riskit eivät ole vakuuttamiskelpoisia, jolloin niitä pitää hallita muiden riskienhallinnan työkalujen avulla. Vakuutuskelpoisuus liittyy näin ollen kyberriskeihin, joiden on oltava vakuuttamiskelpoisia, jotta on voitu lanseerata kybervakuutus. Kybervakuutuksella taas vakuutetaan kyberriskejä yhtenä riskienhallinnan muotona. Näin ollen kaikki taustateoriana toimivat käsitteet linkittyvät toisiinsa joko suoraan tai toistensa välityksellä. Vakuuttamiskelpoisuus taas liittyy riskienhallintaan kyberriskien sekä kybervakuutuksen kautta. Nämä kaikki käsitteet muodostavat yhdessä teoreettisen alustan,

minkä pohjalta tutkimusongelmia tarkastellaan ja mitä vasten empiirisestä osiosta saatuja tuloksia peilataan.

1.4 Tutkimusmenetelmät ja aineisto

Tämä tutkimus on kvalitatiivinen tutkimus. Kvalitatiivisessa tutkimuksessa pyritään tutkimaan kohdetta mahdollisimman kokonaisvaltaisesti ja tarkoituksena on mahdollisimman kokonaisvaltainen tiedonhankinta. Valitsin kvalitatiivisen tutkimustavan, koska aihepiirinä kyberriskit ovat verrattain uusi ja tietoa on rajoitetusta saatavilla. Aihetta on myös helpompi lähestyä kvalitatiivisen tutkimusmenetelmän ja asiantuntijahaastatteluiden kautta, koska näillä menetelmillä saadaan syvällisempää tietoa tutkimusalueesta kuin kvantitatiivisella tutkimuksella. Kvalitatiivisessa tutkimuksessa ollaan kiinnostuneita kielen piirteistä, säännönmukaisuuksien keksimisestä, tekstin tai toiminnan merkityksen ymmärtämisestä sekä reflektioista. Kvalitatiivisessa tutkimuksessa korostuu laadullisten metodien käyttö aineiston hankinnassa, kohdejoukko valitaan tarkoituksen mukaisesti eikä satunnaisotannalla, tutkimussuunnitelma muotoutuu usein tutkimuksen edetessä sekä tapauksia käsitellään ainulaatuisina ja tämän pohjalta tulkitaan aineistoa. (Hirsijärvi, Remes & Sajavaara 2009, 157–161, 135; 181)

Tutkimuksen tarkoitusta voidaan luonnehtia neljän piirteen avulla. Tutkimuksen tarkoitus voi olla kartoittava, kuvaileva, selittävä tai ennustava. Tämän tutkimuksen tarkoitus on kartoittava. Kartoittavan tutkimuksen tarkoituksena on etsiä uusia näkökulmia ja löytää uusia ilmiöitä. Kartoittavassa tutkimuksessa näin ollen selvitetään vähän tunnettuja ilmiöitä ja dokumentoidaan niiden keskeisiä piirteitä. (Hirsijärvi ym. 2009, 138) Koska aihetta ei ole vielä varsinkaan Suomessa tutkittu kovinkaan paljoa, on tämän tutkimuksen tarkoitus kartoittava. Tarkoituksena on saada käsitys tästä vähän tutkitusta aiheesta ja näin ollen luoda pohjaa myös uusille tutkimuksille.

Tutkielman empiirinen osio koostuu asiantuntija haastatteluista. Haastattelu ovat valittu tutkimusmenetelmäksi sillä perusteella, että tutkimusaihe on verrattain uusi ja tutkimustietoa on vähän saatavilla. Haastattelun vastauksien suuntia on myös etukäteen vaikea tietää ja haastateltavien vastaukset voivat olla monitahoisia. Haastattelussa voidaan myös säädellä aineiston keruuta joustavasti ja tilanteen mukaisesti. Haastateltava voi myös kertoa aiheesta enemmän ja vapaammin kuin alustavasti pystytään ennakoimaan, jolloin saatuja vastauksia pystytään sel-

ventämään ja tarvittaessa myös syventämään. Tämä on olennaista, jotta saadaan mahdollisimman kattavasti tietoa tutkittavasta ilmiöstä. Tutkimuksessa ihminen koetaan aktiivisena ja merkityksiä luovana osapuolena. Haastattelun etuna on myös se, että aineistoa voidaan helposti täydentää myöhemminkin haastateltavilta, jos se on tarpeen. (Hirsijärvi ym. 2009, 205–206)

Haastattelut toteutetaan teemahaastatteluina, jolloin haastattelun teemat ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys voivat vaihdella. (Hirsijärvi ym. 2009, 205; 208) Tutkija voi asetella ja esittää kysymykset haastattelun aikana sopivaksi katsomassaan järjestyksessä. Teemahaastatteluja voidaan pitää avoimen – ja lomakehaastattelun välimuotona. Teemahaastattelussa tutkimuksen teemat eli aihepiirit ovat tiedossa, mutta kysymyksillä ei ole välttämättä tarkkaa sanamuotoa tai järjestystä. Se pitääkö kaikille haastateltaville esittää kaikki samat kysymykset ja samassa järjestyksessä on makukysymys ja myös laadullisen tutkimuksen perinteisiin liittyvä kysymys. Yhdenmukaisuuden vaateen aste vaihtelee tutkimuksesta toiseen. Vaihteluväli voi olla jopa avoimen haastattelun tyyppisestä haastattelusta strukturoidusti etenevään haastatteluun. (Tuomi & Sarajärvi 2009, 75)

Teemahaastatteluja käytetään paljon yhteiskuntatieteellisessä tutkimuksessa, koska se vastaa hyvin useita kvalitatiivisen tutkimuksen lähtökohtia. Teemahaastattelut eivät ole kuitenkaan myöskään pelkästään kvalitatiivisessa tutkimuksessa käyttökelpoinen, vaan sitä voi soveltaa myös kvantitatiiviseen tutkimukseen. (Hirsijärvi ym. 2009, 208) Teemahaastattelut valittiin haastattelulajiksi, koska teemahaastattelu antaa jouston varaa sekä mahdollisuuden tarkentaa tai syventää joitakin kysymyksiä ja vastauksia.

1.5 Aikaisemmat tutkimukset ja tutkimuksen rakenne

Kyberriskeihin ja niiden vakuuttamiseen suoraan liittyviä tutkimuksia ei ole aikaisemmin Suomessa tehty. Seuraavat tutkimukset ovat kuitenkin tehty kyberilmiöön liittyen. Lönnqvist Irina on kirjoittanut vuonna 2013 opinnäytetyönsä aiheesta Elämmekö kyberriskiyhteiskunnassa? Tutkimuksessa hän tarkastelee kyberilmiötä Ulrich Beckin riskiyhteiskunnan käsitteen kautta. Riskiyhteiskunnan ajatus on, että ihminen luo tietoisesti ja tiedostamatta ympärilleen riskejä, joita on vaikea hallita. Nykypäivänä riskiyhteiskunta on muuttunut yhä teknologisemmaksi. Tässä tutkimuksessa hän soveltaa Ulrich Beckin riskiyhteiskunnan käsitettä kyberilmi-

öön. Loppupäätelmänä Lönnqvist toteaa, että on siirrytty kyberriskiyhteiskuntaan. Limnell Jarno on tutkinut kyber-ilmiötä tutkimuksessaan, Kyber rantautui Suomeen. Tutkimuksessa hän on pyrkinyt selvittämään, milloin kyber-puhe ja -kieli ovat tulleet suomalaiseen hallinnolliseen turvallisuusajatteluun. Limnellin mukaan Kyber-käsitteen hallinnollisen institutionalisoitumisen sekä läpimurron Suomeen voidaan katsoa tapahtuneen Suomen Kyberturvallisuusstrategian myötä, joka ilmestyi vuoden 2013 alussa.

Tämän tutkimuksen tärkeyttä voidaan perustella sillä, että vastaavanlaista tutkimusta ei ole Suomessa aikaisemmin tehty. Tutkimuksen aihe on myös todella ajankohtainen ja merkittävä niin liiketaloudellisesti kuin yhteiskunnallisestikin. Kybervakuutusmarkkinat ovat kasvaneet lähivuosina merkittävästi niin Suomessa kuin maailmanlaajuisesti. Tutkimus noudattaa perinteistä IMRD- rakennetta. Tutkimus koostuu kuudesta pääluvusta ja niiden alaluvuista. Ensimmäinen pääluku on johdanto, jossa kerrotaan yleisesti kyberilmiöstä ja johdatellaan tutkimuksen aiheeseen. Lisäksi kerrotaan tutkimusongelmat ja rajaukset, tutkimuksen teoreettinen viitekehys, tutkimusmenetelmät ja aineisto sekä sivutaan aikaisempia tutkimuksia. Johdanto kappaleen jälkeen tutkimuksessa esitetään teoreettinen osuus, joka jakautuu kolmeen päälukuun. Ensimmäisessä pääluvussa perehdytään kyberriskeihin sekä niiden luonteeseen. Toisessa pääluvussa käsitellään riskienhallintaa, joka luo pohjaa koko tutkimukselle. Kolmannessa pääluvussa taas perehdytään kybervakuutukseen sekä kybervakuutusmarkkinoihin maailmanlaajuisesti. Viidennessä pääluvussa siirrytään tutkimuksen empiiriseen osioon, jossa käydään tutkimuksen haastattelut läpi. Kuudennes luvussa tehdään johtopäätökset ja yhteenveto, jonka lisäksi arvioidaan tutkimuksen luotettavuutta sekä esitetään jatkotutkimusehdotukset.

2 KYBERRISKIT

2.1 Kyberilmiö ja sen määrittely

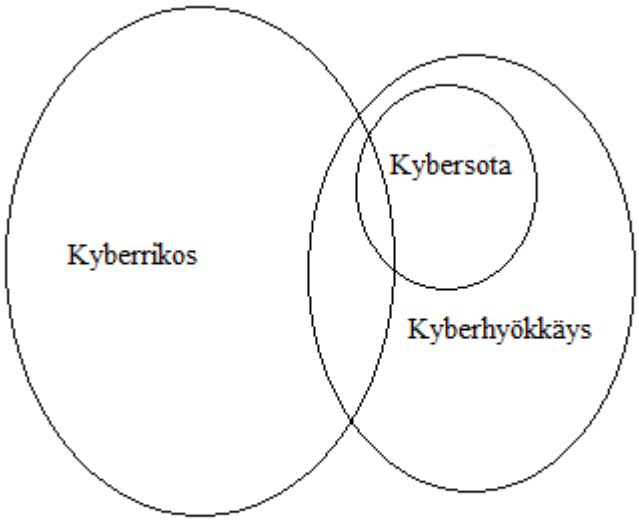
Teknologia ja digitalisoituminen ovat uusien mahdollisuuksien myötä tuoneet maailmaan myös uudenlaisia riskejä, joita kutsumme kyberriskeiksi. Kyberriskit ovat kasvava ilmiö ja yhä useampi yritys maailmanlaajuisesti altistuu näille riskeille, koska yhä useampi yritys toimii inter-

netissä tai vähintäänkin osa yrityksen palveluista. Kyberriskeillä tarkoitetaan informaatioteknologia järjestelmissä tapahtuvia häiriöitä, joidenka seurauksina yritys kärsii kuljetukseen, maineeseen tai varallisuuteen liittyviä tappioita. Tällaiset riskit voivat realisoitua esimerkiksi, kun yrityksen ulkopuolinen henkilö pääsee käsiksi tietojärjestelmiin tarkoituksenaan vakoilla, kiristää tai varastaa asiakastietoja yhtiöltä. Riski voi myös realisoitua vahingon tai tahattoman IT turvallisuuteen liittyvän teon johdosta sekä jos tietoturvallisuuteen liittyvät järjestelmät ovat puutteelliset. (Irm 2014, 8)

Kyber-tapahtumat ovat hyvin laaja käsite ja kyberriskit ovat osa tätä käsitettä. Kyber-tapahtumat pitävät sisällään kyberhyökkäykset, kyberrikokset sekä kybersodankäynnin. Kyberhyökkäys tarkoittaa ainutlaatuista uhkaa, mikä muodostuu kyberteknologiasta ja sen käytöstä. Kyberhyökkäys muodostuu tapahtumista, joilla on tarkoitus heikentää tietoverkkojen toimimista poliittisessa tai kansallisessa tarkoituksessa. Jotta voidaan ymmärtää kyberhyökkäyksen käsitettä, on ymmärrettävä sen erot kyberrikokseen sekä myös kybersodankäyntiin. Kyberrikos on kaikista laajin käsite, mutta sille ei ole universaalisti tunnistettua määritelmää. Kyberrikos on kuitenkin yleisesti ymmärretty laittomaksi teoksi, joka toteutetaan käyttämällä tietokonepohjaisia keinoja. Se voidaan myös ymmärtää miksi tahansa rikokseksi, joka on toteutettu käyttämällä tietokonetta tai internetiä. Kyberrikos ei ole siis tehty poliittisessa tai kansallisessa tietoverkkojen heikentämisen tarkoituksessa, toisin kuin kyberhyökkäys. (Hathaway 2012, 826, 833–834)

Suurin osa kyberrikoksista ei ole samaan aikaan osa kyberhyökkäystä tai kybersotaa. Kyberrikos on vain kyberrikos, kun yksityishenkilö suorittaa rikoslainalaisen toimenpiteen tietokoneen välityksellä. Kyberrikos voi olla esimerkiksi tilanne jossa yksityishenkilö murtautuu pankin tietojärjestelmiin ja heikentää näin niiden suorituskykyä. Toimenpiteen tarkoituksena on saada varallisuutta, mutta sitä ei suoriteta poliittisessa tai kansallisessa tarkoituksessa, jolloin se on kyberrikos eikä kyberhyökkäys. Kyberrikos voi myös olla osa kyberhyökkäystä, kun yksityishenkilö suorittaa laittoman teon tietokoneen välityksellä, heikentää tietoverkkoa ja hänellä on poliittinen tai kansalliseen turvallisuuteen liittyvä tarkoitus. Kybersodankäynti taas tarkoittaa, että rikoksen tekijänä on yksityishenkilön sijaan valtio. Kybersodankäynti sisältää aina kyberhyökkäyksen ehdot, mutta kaikki kyberhyökkäykset eivät ole kybersotaa. Kybersota on aseistettu hyökkäys. (Hathaway 2012, 835) Haktivismi termi taas tulee hakkeroinnin ja aktivismin yhdistämisestä. Eli tietojärjestelmien hakkeroimisesta poliittisessa tarkoituksessa. (Quigley, Burns & Stallard 2015, 110) Tutkimusaineistossa ja kansainvälisissä artikkeleissa termi

kyberhyökkäys toistuu usein ja sitä käytetään enemmän kuin kyberrikos termiä. Monissa tutkimuksissa on käytetty kyberhyökkäys termiä, vaikka kyseessä ei ole ollut kyberrikos joka on suoritettu poliittisessa tai kansallisessa tarkoituksessa. Puhtaista kyberrikoksista puhutaankin tutkimuksissa usein kyberhyökkäyksinä, joten termiä käytetään myös tässä tutkimuksessa paljon. Varsinainen kybersodankäynti ja sen tutkiminen on jätetty tämän tutkimuksen ulkopuolelle. Seuraavassa kuviossa on konkretisoitu kyberrikoksen, kyberhyökkäyksen sekä kybersodankäynnin välisiä yhtäläisyyksiä ja eroja.



Kuvio 2. Kybertapahtumat. Kybertapahtumilla voidaan tarkoittaa niin kyberrikosta, kybersotaa kuin kyberhyökkäystäkin.

Suomeen perustettiin kyberturvallisuusstrategia vuonna 2013, kun Yhdysvalloissa kyberturvallisuusstrategia perustettiin jo vuonna 2003. (Keegan 2014) Quigley ym. (2015, 115) mukaan kyberilmiöstä käytettävissä metaforissa pitäisi olla tarkkana. Esimerkiksi kyberilmiöstä käytetty metafora ”taistelukenttä” on ylikäytetty, epätarkka ja usein harhaanjohtava. Valtiolla on iso rooli kyberriskeistä tiedottamisessa ja valtion pitäisikin olla tarkempi siinä, millä termeillä kyberilmiöstä puhuu. Quigley ym. ehdottavat kyberilmiöstä puhumista taistelukentän sijaan Amerikan villinä läntenä, jossa on vähän sääntelyä ja harkittuja mahdollisuuksia sekä vaaroja. Vaikka kyberilmiö on tuonut aivan uudenlaisia riskejä, on se myös mahdollistanut monia uusia teknologioita sekä palveluita.

2.2 Haittaohjelmat

European Union Agency for Network and Information Security on raportoinut vuoden 2015 merkittävimmät 15 kyberuhkaa niiden merkittävyys ja yleisyys järjestyksessä: 1) haittaohjelmat, 2) internetpohjaiset hyökkäykset, 3) internet sovellus hyökkäykset, 4) bot verkot, 5) palvelunestohyökkäykset 6) fyysiset varkaudet tai vahingoittamiset, 7) sisäpiiriuhkat, 8) verkkourkinnat, 9) roskapostit, 10) riisto, 11) datamurrot, 12) identiteettivarkaus, 13) informaatiovuoto, 14) kiristysohjelmat ja 15) kybervakoilut. (www.enisa.com) Teknologian kehitys lisää myös kyberrikosten kehitystä, kun uusia tapoja tehdä kyberrikoksia syntyy ja niiden jäljitettävyys heikkenee jatkuvasti. Kaikista yleisimmät hyökkäykset tähän asti ovat kuitenkin syntyneet perinteisistä kyberuhkista. Palvelunestohyökkäys (Denial of service, DoS) on verkkohyökkäys, jossa pyritään estämään verkkosivujen käyttö. Tietoverkkoon kohdistetaan niin paljon liikennettä, että se ei pysty palvelemaan asiakkaitaan. Haittaohjelma on yleisnimitys tietokoneohjelmille, jotka aiheuttavat ei-toivottuja tapahtumia tietokoneessa ja sen järjestelmissä. Hyökkääjän tarkoituksena on vaarantaa datan luotettavuus, saatavuus sekä koskemattomuus. (Bendovschi 2015, 25)

Yleisimpiä haittaohjelmia ovat virukset, madot, troijalaiset, takaportit, kiristysohjelmat, vakoiluohjelmat, verkkourkinta sekä käyttäjän manipulointi. *Madot* leviävät ilman isäntäohjelmien apua esimerkiksi tietoturva-aukon välityksellä tai huijaamalla käyttäjän suorittamaan itsensä. *Troijalainen* on tietokoneohjelma, joka näyttää tekevän muuta kuin oikeasti tekee. Troijalaiset voivat myös käynnistää viruksen tai muun haittaohjelman ja käyttää hyväkseen järjestelmän haavoittuvuutta. *Takaportti* on tietotekniikassa rakenne, joka mahdollistaa ulkopuolisen pääsyn tietotekniikan välityksellä laitteeseen ohittamalla tietoturvamekanismit. *Kiristysohjelma* lukitsee tietokoneen käytön, kunnes tietty rahasumma on maksettu. *Vakoiluohjelma* taas on ohjelmisto, joka vakoilee käyttäjän toimintaa yksittäisellä koneella tai verkossa ja pystyy lähettämään tiedot kolmansille osapuolille. Vakoiluohjelmia ovat muun muassa näppäimistölukijat, selainkaappaajat sekä haitalliset mainosohjelmat. *Verkkourkinta* (phishing) on tekniikka, jolla pyritään saamaan luottamuksellisia tietoja kuten tilitietoja, esiintymällä tietoon oikeutettuna henkilönä. *Käyttäjän manipulointi* (social engineering) on toimintaa, jolla yritetään saada käyttäjä luottamaan hyökkääjään tarpeeksi ja näin ollen antamaan pääsy salattuihin tiedostoihin. PwC:n tutkimuksen mukaan kyberrikokset ovat kehittyneen niin laajalle, että noin 117 000 hyökkäystä tapahtuu päivässä maailmanlaajuisesti. (Bendovschi 2015, 25)

Kyberhyökkäykset voivat olla syntaktisia tai semanttisia tai näiden sekoituksia niin kutsuttuja yhdistettyjä hyökkäyksiä. Syntaktiset hyökkäykset hyödyntävät teknillisiä haavoittuvuuksia ja heikkouksia kyberrikoksen tekemisessä. Tästä esimerkkinä on juuri haittaohjelman asentaminen datan varastamisen tarkoituksessa. Semanttiset hyökkäykset taas hyväksikäyttävät sosiaalisia heikkouksia henkilökohtaisten tietojen saamiseen eli niissä tehdään verkkourkintaa. Tällaisia ovat esimerkiksi huijauspyyntöjen lähettäminen sekä verkkokauppapetokset. Yhdistetyt hyökkäykset sisältävät tietojen kalastelua eli verkkourkintaa, joka on tänä päivänä verrattain helppoa sosiaalisen median avulla sekä ne myös hyödyntävät teknillisiä haavoittuvuuksia. Tutkimusten mukaan pankki- ja finanssisektori ovat olleet yksi suosituimmista verkkourkinnan kohteista viime vuosien aikana. IBM X-Forcen raportin mukaan finanssilaitokset olivat vuonna 2009 kohteena 60 prosenttia ja vuonna 2010, 50,1 prosenttia kaikista verkkourkinta hyökkäyksistä. Verkkourkinta oli yksi viidestä kalleimmasta kyberrikoksesta vuosina 2010 ja 2011. Verkkourkinnan uhreina on sekä yksilöitä että organisaatioita julkiselta sekä yksityiseltä sektorilta. Vaikka organisaatio kärsii tappion verkkourkinnan seurauksena, voidaan todellisena uhrina pitää kuitenkin asiakasta, joka saa huijausviestin ja on näin ollen tungettelun kohteena. Huijauksien kohteena ovat myös usein johtajat sekä muut organisaatioiden vaikutusvaltaiset henkilöt, joiden kautta rikolliset yrittävät saada yhteyden esimerkiksi yrityksen nettipankkiin. (Choo & Kwang 2011, 724)

Sen lisäksi, että organisaatioiden on varauduttava ja otettava huomioon näiden uhkien suora vaikutus organisaatioon on huomioitava myös se, jos riskit toteutuvat toimitusketjussa toiselle organisaatiolle tai avainasiakkaalle. Nykyään yritykset käyttävät myös yhä enenevissä määrin pilvipalveluita. Pilvipalveluiden käyttö ei itsessään kuitenkaan lisää tai vähennä yrityksen riskiprofiilia, tehokkaasti kontrolloitu ja valvottu ympäristön siirto pilvipalveluun säilyy kontrolloituna, jos kontrollit pysyvät tehokkaana. Huonosti kontrolloitu ympäristö tuo mukanaan taas riskejä. (Irm 2014, 8)

2.3 Kyberrikokset numeroina

Bendovschin (2015) tutkimuksen mukaan viimeisen edeltäneen kolmen vuoden aikana on tapahtunut 15 miljoonaa tunnistettua kyberhyökkäystä maailmanlaajuisesti. Tutkimuksen mukaan tietomurtojen pohjimmaisista syistä alle 50 prosenttia oli aiheutunut rikosperäisistä hyök-

käyksistä. Tietomurtojen syyt jakautuivat kolmeen tekijään: 1) tarkoitetut suunnitellut hyökkäykset, 2) inhimillisen virheen aiheuttamat hyökkäykset sekä 3) järjestelmien haavoittuvuuksista johtuvat hyökkäykset. Näin ollen, kun hyökkäys onnistuu, on se vain osittain hyökkääjän osaamisesta kiinni ja osittain taas uhrin haavoittuvuuksista kiinni, joita voivat olla virheet ohjelmissa, inhimilliset virheet sekä liian alhainen tietoturvataso.

Application Vulnerability Trends Raportin (2014, 3) mukaan 96 prosentista analysoiduista sovelluksista on yksi tai useampia isoja haavoittuvuuksia. Keskimääräinen haavoittuvuuksien määrä per sovellus oli 14. Suurin osa hyökkäyksistä on tullut Yhdysvalloista, Venäjältä, Hollannista, Saksasta, Vietnamista, Romaniasta, Canadasta ja Ranskasta ja suurin osa uhreista taas on ollut Yhdysvallat, Venäjä, Iso-Britannia, Saksa, Italia, Ranska ja Hollanti. Korrelaatiota löytyy eri kyberilmiöiden sekä toimialojen välillä. Julkinen sektori on todennäköisemmin kybervakoilun, -sodan ja haktivismin kohteena, kun taas kyberrikokset koskevat kaikkia toimialoja. Lisäksi mobiililaitteiden hakkeroiminen on lisääntynyt jatkuvasti. Älypuhelimet käyttävät monia sovelluksia, ovat jatkuvasti yhteydessä internettiin, niitä suljetaan harvoin ja ne sisältävät paljon henkilökohtaisia tietoja.

Mobiilihaittaohjelmat ovat jo nykypäivää, mutta niiltä suojautuminen on vielä lapsen kengissä. Anti-virus ohjelmat älypuhelimille ovat harvassa, älypuhelimien virusten syntymisestä ja kasvusta huolimatta. Kuitenkin IT yhtiöt kiinnittävät yhä enemmän huomiota tähän kasvavaan ongelmaan ja esimerkiksi McAfee ja VirusScan ovat alkaneet tarjota anti-virus aplikaatioita älypuhelimiin. (Choo 2011, 722)

PwC:n Englannissa tehdyn tutkimuksen mukaan yritykset ovat yhä tietoisempia kyberuhkista ja kuinka niiltä voidaan suojautua. Tutkimukseen osallistui kaikkiaan yli 600 yritystä kaikilta toimialoilta. 90 prosenttia isoista yhtiöistä ja 74 prosenttia pienistä yrityksistä olivat kärsineet tietomurroista vuonna 2015. Luvut ovat nousseet vuoden 2014, 81 ja 60 prosentista. 59 prosenttia vastaajista odotti tietomurtojen lisääntyvän seuraavan vuoden aikana. Tietomurroista aiheutuvat kustannukset ovat myös selvästi kasvaneet verrattuna vuoteen 2014. Suurimman tapahtuneen tietomurron kustannukset isoilla yhtiöllä olivat 1,46 – 3,14 miljoonaa puntaa vuonna 2015, kun vuonna 2014 ne olivat 600 000 – 1,5 miljoonaa puntaa. Pienillä yrityksillä kustannukset olivat nousseet 75 000 – 310 000 punnan suuruusluokkaan 65 000 – 115 000 punnan suuruusluokasta. Kyberhyökkäysten määrä sekä niistä aiheutuvat kustannukset ovat siis kohonneet vuodesta 2014 (PwC Information security breaches surveys 2015, 6-8)

PwC:n tutkimukseen osallistuvat yritykset kärsivät eniten viruksien ja haittaohjelmien aiheuttamista tartunnoista. Yritykset kärsivät myös työntekijöidensä aiheuttamista tietosuojaan liittyvistä tapahtumista sekä ulkopuolisten aiheuttamista tietoverkkojen hakkeroinnista. Esimerkki Iso-Britannian valtion yrityksen työntekijä paljasti inhimillisestä virheestä johtuen arkaluonteista tietoa, millä oli vakavia vaikutuksia yritykseen ja sen maineeseen. Vuoteen 2014 verrattuna yhä useampi yritys kärsi näistä riskeistä. (PwC Information security breaches surveys 2015, 11)

Viimeisen viiden vuoden aikana merkittävimpiä tietomurtoja ovat olleet Yhdysvaltalaisen kolmanneksi suurimman kauppaketjun Targetin tapaus, jossa varastettiin 70 miljoonan asiakkaan tiedot, Neiman Marcusin tapauksessa 40 miljoonan asiakkaan tiedot, LivingSocial 50 miljoonan asiakkaan tiedot sekä Applen tapaus, jossa varastettiin 12 miljoonan asiakkaan tiedot. Näiden lisäksi tietomurron kohteeksi joutuivat 7-Eleven, JCPenney, Dow Jones, NASDAQ ja JetBlue joiden asiakkaiden tietoa varastettiin yhteensä 160 miljoonaa kappaletta. 2013 syyskuusta lähtien kiristysohjelmahyökkäykset, jotka on tehty CryptoLocker troijalaisella tai muulla troijalaisella, mitkä estävät yritysten tai yksilöiden pääsyn tallennettuun dataan, ovat lisääntyneet. (Zelle & Whitehead 2014, 147)

Kyberympäristö muuttuu jatkuvasti ja näin ollen siihen liittyvät riskitkin ovat jatkuvasti muutoksessa. Organisaatioiden haasteena on pysyä mukana muutoksessa ja ylläpitää reagointikykyä muutoksiin sekä uusiin mahdollisuuksiin ja uhkiin. Sosiaalinen media on tuonut organisaatioille omat mahdollisuutensa mutta myös uhkat. Euroopan komission arvioin mukaan yli miljoonaa ihmistä joutuu kyberrikoksen uhriksi päivittäin. Kyberriskit eivät koske myöskään vain suuria yhtiöitä, finanssitaloja tai tunnettuja brändejä vaan myös pieniä yrityksiä. Kasvavan trendin mukaan rikolliset ottavat kohteekseen yhä enemmän pieniä, ei niin hyvin suojattuja, yrityksiä. (Irm 2014, 8) Pieniä yhtiöitä on enemmän kuin isoja, joten kyberrikollisille on myös luonnollisesti enemmän kohteita pienten yritysten joukossa. Pienillä yrityksillä on myös niukemmat resurssit ostaa suojaa kyberriskejä vastaan ja näin ollen ne ovat haavoittuvampia. Heillä on myös vähemmän resursseja tarjota tietoturvakoulutusta työntekijöilleen. (Voelker 2015, 45)

Bienerin ym. (2015, 134) mukaan Euroopassa 25 prosenttia yrityksistä ei ole edes tietoisia, että tämän tyylinen riski on olemassa. Allianzin Risk Barometer 2015 tutkimuksen mukaan kyberriski on riski, johon yritykset ovat vähiten varautuneet. Kyberriski on myös aliarvioiduin riski, jonka yritykset kohtaavat. Kyberriski on myös nostanut asemiaan top 10 riskeissä viimeisen kahden vuoden aikana, se on noussut viidennestätoista sijasta viidenteen. Tutkimuksen mukaan

Kanada, Iso-Britannia ja Etelä-Afrikka pitivät kyberriskejä suurimpina liiketoiminnan riskeinä tällä hetkellä. Suurin taloudellisen tappion aiheuttaja kyberriskin toteutumisen jälkeen oli maineen menetys. Tämän jälkeen tulivat liiketoiminnan keskeytyminen ja toimitusketjun häiriintyminen sekä korvausvaatimukset tietomurron jälkeen. Isoin syy mikä estää yhtiöitä suojautumaan paremmin kyberriskejä vastaan, on tiedon ja osaamisen puute. Seuraavia syitä olivat ne, että yritys ei ole vielä täysin arvioinut riskin rahallista arvoa sekä budjettiin liittyvät rajoitteet. Suurin osa muista maailman valtioista pitivät liiketoiminnan keskeytymisen riskiä suurimpana liiketoiminnan riskinä. Kyberriskit kuitenkin itsessään lisäävät liiketoiminnan keskeytymisen riskiä. (Allianz, 2015)

Digitalisaatio on muuttanut ja tulee jatkuvasti muuttamaan liiketoiminnan ympäristöä. Yrityksiä eniten pelottavat asiat digitalisoitumisessa ovat kyberhyökkäysten kehittyneisyys, datapetos tai varkaus sekä kriittisen infrastruktuurin kaatuminen. Digitalisaation myötä yhä useammat yritykset linkittyvät internettiin ja kyberavaruuteen. Kyberriskit onkin listattu myös suurimmaksi pitkän aikavälin riskiksi. (Allianz, 2015)

2.4 Uudenlaiset kyberriskit

Internet of things eli asioiden internet lisää kyberriskejä myös tulevaisuudessa ja ennusteen mukaan arviolta 50 biljoonaa keksintöä tulee olemaan yhdistettynä internettiin vuoteen 2019 mennessä. (Bendovschi 2015, 26) Kyberriskit eivät koske enää pelkästään datan varastamista ja aineetonta omaisuutta vaan myös fyysisiä laitteita. Kyberrikolliset pystyvät hakkeroimaan tuotantolaitosten laitteistoja ja tämän johdosta aiheuttamaan suuria fyysisiä tuhoja yrityksille. Esimerkiksi 2014 saksalaisen terästehtaan tuotannon kontrollijärjestelmiin murtauduttiin ja niitä manipuloitiin niin, että sulatusuuni ei sulkeutunut kunnolla, mikä aiheutti suurta fyysistä tuhoa yritykselle. Kyberriskeihin liittyvät omaisuusvahingot ovat jatkuvasti kasvava uhka. Vakuutustoimialalla tämä uusi vahingoittamisen muoto on nyt pinnalla ja niin kybervakuutus kuin omaisuusvahinko osastot mieltävät tämän alueen vakuutuspiirinsä ulkopuolelle. Omaisuusvahinkoja korvaavat vakuutukset on tarkoitettu kattamaan fyysisiä vahinkoja, kun taas kybervakuutus korvaa aineettomia vahinkoja. Jotkut vakuutusyhtiöt ovat yrittäneet luoda kokonaan uutta kybertuotetta, joka kattaisi myös näitä fyysisiä vahinkoja. Kybervakuutuksen myyjät kuitenkin tietävät kyberriskeistä enemmän kuin muut, mutta heillä ei ole välttämättä kokemusta omaisuusvahinkojen hinnoittelusta. (Smith 2016)

Vahinkovakuutusyhtiöt ovat huolissaan systeemiriskistä sekä riskin keräytymisestä. Toisinkuin muut uhkat, kyberriskejä ei voi rajoittaa. Kyberriskeillä ei ole fyysisiä rajoja, minkä vuoksi ne haastavat mallinnus skenaariot. Mallinnuksissa ei voida sanoa, mikä on suurin mahdollinen tuho tai minne asti riskin toteutuminen tulisi vaikuttamaan toisinkuin esimerkiksi maanjäristyksessä. Kyberriskeistä ei ole saatavilla aktuaaridataa useiden vuosien takaa, joten mallinnuksissa on otettava esimerkkiä muista hankalista mallinnustilanteista kuten maanjäristyksestä. Aon on yhteistyössä RMS:n kanssa tehnyt mallin, joka on lanseerattu helmikuussa 2016. Vakuutusmarkkinoilla käydään nyt keskustelua olisiko kybervakuutusta vai omaisuusvakuutusta uudistettava niin, että ne kattaisivat kyberriskeistä johtuvat fyysiset vahingot. Vakuutusyhtiöiden kyber- sekä omaisuusvahinko osastojen siilot olisi purettava ja tehtävä yhteistyötä näiden osastojen välillä, jotta saadaan kehitettyä yhdistetty vakuutustuote, joka lainaa omaisuusvahinkojen aktuaaridataa hinnoitteluun kyberriskien tuntemuksella, jotta voidaan identifioida riskit ja potentiaaliset vahingot. AIG on esimerkiksi jo kehittänyt kybervakuutus tuotteen AIG CyberEdge PC, joka suojaa myös kyberhyökkäyksistä aiheutuneilta fyysisiltä vahingoilta. (Smith 2016)

2.5 Kyberriskien kustannukset

Kun organisaatio miettii investoimista tietoturvaan, tulee kysymykseen tietenkin kustannukset niin kuin jokaisessa päätöksentekotilanteessa. Yleensä yritykset pohtivat onko ylipäätään kannattavaa investoida kyberturvallisuuteen. Yritykset painivat yleensä monien kysymysten äärellä, joita ovat muun muassa, paljonko pitäisi investoida kyberturvallisuuteen tai sen kontrolleihin? Entä paljonko vakava tietomurto tulisi kustantamaan yritykselle? Tutkimusyhtiö Gartner:in mukaan organisaatiot tulevat kuluttamaan 76.9 biljoonaa dollaria maailmanlaajuisesti kyberturvallisuuteen vuonna 2015, kun vuonna 2014 luku oli 71.1 biljoonaa dollaria. (Mccollum 2015, 28)

Kybertapahtumat ovat nykyään niin laajalle levinneitä, että niihin liittyviä kustannuksia on vaikea täsmällisesti arvioida ja ne hyväksytäänkin yhä enenevissä määrin osana riskiä, joka aiheutuu normaalista liiketoiminnasta. Suorat kustannukset voivat liittyä asiakkaiden informointiin, murron jälkeisiin varmistustoimenpiteisiin, sääntelyyn liittyviin sakkoihin, PR-tiedottamiseen sekä teknisten analyysien korjaamiseen ja parantamiseen. Kyberuhkien laajentumisen myötä monet johtajat kohdistavat yhä suuremman osan budjetista tietoturvaan ja ostavat kybervakuutuksen. Se ei kuitenkaan yksinään riitä vaan on samalla luotava entistä kokonaisvaltaisempi

kyberriskienhallinta ohjelma. Kyberriskejä on tarkasteltava laajemmin ja ymmärrettävä, että datavarkaus ei ole ehkä se kaikkein vahingoittavin tekijä kyberrikoksen sattuessa organisaatiolle. Operationaalisella tuholla sekä organisaation sekasorrolla voi olla paljon pahempi vaikutus organisaatioon, kuin datavarkaudella. (Mossburg 2015, 77)

Useat tekijät vaikuttavat kyberhyökkäyksistä aiheutuneiden kustannusten epätavallisen suureen kasvuun. Niiden joukossa ovat kyberhyökkäysten lisääntyminen, tietosuojabudjettien pienentäminen sekä epäonnistunut kyberriskien käsittäminen osana koko yrityksen käsittävää strategista riskienhallintaa. (Gregg 2010, 61)

Deloitten tekemän tutkimuksen mukaan on monia kustannuksia, joihin yritykset eivät ole osanneet varautua. 1) Lähempi liiketoiminnan tarkastelu: suoraan murrosta tapahtuvien sakkojen lisäksi tietomurto voi laukaista laajemman organisaation tarkastuksen, josta voi taas seurata lisää sakkoja, jos laajempia laiminlyöntejä ilmaantuu. 2) Korkeammat kybervakuutusmaksut: yhtiöt, jotka ovat kärsineet julkisesti ilmi tulleen tietomurron, kohtaavat todennäköisesti tulevaisuudessa korkeammat vakuutusmaksut. 3) Murron kesto voi vaikuttaa myös yrityksen brandiin sekä maineeseen. 4) Oikeudenkäyntikulut voivat nousta vielä vuosiakin murron tapahtumisen jälkeen, johtuen korvausvaatimuksista. 5) Tietomurron tapahtuminen voi aiheuttaa myös yrityksen luottoluokituksen madaltumisen, mikä taas johtaa lainarahan hinnan nousuun. Deloitten tutkimuksessa vertailtiin yrityksiä, jotka olivat kärsineet tietomurrosta ja yrityksiä, jotka eivät olleet. Keskimäärin murrosta kärsineiden yritysten luottoluokitus laski yhdellä tasolla verrattuna yrityksiin, jotka eivät olleet kärsineet tietomurroista. Esimerkiksi tutkimuksen teon aikana korkotaso 10 vuoden A-luokituksen valtionvelkakirjalle oli keskimäärin 3,44 prosenttia, kun taas BBB-luokitukselle se oli 4,13 prosenttia. Tässä tapauksessa siis A luokasta alentuminen BBB luokkaan aiheuttaisi ylimääräisen 3.6 miljoonan kustannuksen 100 miljoonan dollarin projektin elinaikana. (Mossburg 2015, 77) Lisäksi yrityksen, joka on kärsinyt kyberhyökkäyksestä ja se on tullut julkisuuteen, osakkeiden arvot laskivat ainakin lyhyellä aikavälillä. Tämä johtuu sidosryhmien heränneestä epäluulosta yrityksen tietoturvallisuuden tasoa kohtaan. (Bandyopadhyay, Mookerjee & Rao, 2009, 69)

Riippuen toimialasta tietomurrolla voi olla vakavia vaikutuksia maineeseen ja tätä kautta myyntiin ja liikevaihtoon. Sillä voi myös olla vaikutusta neuvotteluasemaan kauppiaiden kanssa sekä sopimuksien tekoon kolmansien osapuolien kanssa. Kyberrikos voi näin ollen vaikuttaa yrityksen koko markkina-asemaan. Department of Homeland Security’s Industrial Control Systems

Cyber Emergency Response Team julkaisemassa Monitor uutiskirjeessä dokumentoidaan selkeästä kyberhyökkäysten noususta, joissa kohteena ovat teollisuusyritysten kontrollit energia-alalla. Koneiden kytkeminen tietoverkkoon aiheuttaa näin lisää riskejä tuotannon prosesseihin, kuljetus systeemeihin sekä muihin kriittisiin infrastruktuureihin. (Mossburg 2015, 78–79)

Aikaisemmin mainittu, Target kauppaketjuun tehty tietomurto, aiheutti yhtiölle paljon kustannuksia. Arvioidut kustannukset tästä tietomurrosta olivat noin biljoona dollaria. Vuonna 2007 TJX kärsi tietomurrosta, jossa 45.6 miljoonaa luotto-sekä pankkikortti tietoja sekä pankkitili tietoja varastettiin 18 kuukauden aikana. TJX yritys oli tietomurron jälkeisten seuraavien kolmen kuukauden aikana kuluttanut jo 5 miljoonaa dollaria tiedottamalla asiakkaille, joita asia mahdollisesti koski, palkkaamalla ulkopuolista apua arvioimaan varastetun datan määrää sekä käsittelemään aiheeseen liittyvää mediakohua. Lisäksi kustannuksia syntyi, kun yritys joutui palkkaamaan asiantuntijoita puolustamaan yritystä oikeustapauksissa sekä parantamaan tietosuojaansa. Yhdeksän kuukauden jälkeen tietomurrosta aiheutuneet jälkiseuraukset tulivat kustantamaan yhteensä 265 miljoonaa dollaria. TJX käytti miljoonia sisäisiin tarkastuksiin ja merkittäviä summia sovitteluun asiakkaidensa kanssa. TJX tarjosi kolmen kuukauden ilmaiset luotto seuranta palvelut asiakkaille, joiden tiedot oli varastettu. Lisäksi he pitivät kolmen päivän asiakastapahtuman, jossa asiakkaat saivat 15 prosentin alennuksen kaikista tuotteista, käteishyvityksiä sekä ostosetuseteleitä. (Zelle & Whitehead 2014, 152)

Deloitte on listannut talousjohtajien viisi askelta kyberturvallisuuteen, jossa pitää ottaa laajempi ja riskiperusteinen näkemys kybertapahtumiin. Ensinnäkin kaikkiin uusiin projekteihin on huomioitava kyberriskit. On mietittävä lisääkö toimi organisaation altistumista kyberriskeille ja miten kyberriskin toteutuminen vaikuttaisi uuden projektin menestymiseen. Toiseksi kyberriski pitäisi integroida osaksi strategista suunnittelua. Riskienhallintajohtajien tulisi arvioida mahdolliset kulut ja vaikutukset, jos kyberriski toteutuu. Tämä auttaa tekemään parempia päätöksiä riskinottohalusta sekä siitä, miten paljon investoidaan riskin vähentämiseen. Kolmanneksi kyberturvallisuuden rahoitusta pitäisi katsoa eri perspektiiveistä ja investoinnit pitäisi linjata suoraan yhtiön top riskeiksi. On oltava selvillä, miten budjetti vastaa kyberriskeiltä suojautumisen tarpeeseen sekä riskin toteutuessa syntyviin kustannuksiin. Neljänneksi tulisi uudelleen arvioida vakuutusosasto osaksi kyberriski ohjelmaa. On oltava kartalla siitä, kuinka suuri osa riskistä siirretään. Viidenneksi tulisi etsiä osallistujia simulointeihin, jossa testataan yhtiön kykyä reagoida kybertapahtumiin. Harjoitukset auttavat ymmärtämään, miten kybertapahtumat voivat

levitä ja miten oman organisaatio selviäisi tapahtumasta. Talousjohtajilla on hyvät mahdollisuudet vaikuttaa toimitusjohtajien tietämykseen kyberriskeistä ja niiden vaikutuksista organisaation suorituskykyyn. (Mossburg 2015, 79)

2.6 Kyberriskien arviointi sekä pienentäminen

Kyberriskien tunnistaminen ja arviointi ovat tärkeässä roolissa niiltä suojautumisessa. (Nierengarten 2006, 24) Väliä ei ole niinkään, sillä millaisen tietomurron kohteeksi yritys on joutunut vaan sillä, miten ja millaisessa ajassa tietomurto on huomattu ja tunnistettu. Tietoturvatutkimus yrityksen Ponemon Institute:n mukaan isoilta organisaatioilta kesti keskimäärin 206 päivää havaita tietomurto. Tietoturva yritys Trustwave:n mukaan yli 71 prosenttia tapahtumista jää havaitsematta. Lisäksi ISACA ja RSA konferenssin suorittaman tutkimuksen mukaan alle puolet tutkituista IT-ammattilaisista ja IT-tarkastajista olivat sitä mieltä, että heidän yrityksensä voisi havaita sekä vastata vakavaan tietomurtoon. Monet johtajista ovat kääntymässä sisäisen tarkastuksen puoleen, jotta organisaatiolla olisi tarvittavat ominaisuudet tietomurtojen löytämiseksi ja niihin vastaamiseksi. Vuonna 2015 kyberriski on noussut ensimmäistä kertaa top 10 ensisijaisten riskien joukkoon numerolle 9. Aon Global Risk Management Survey:n mukaan. Eri tilastojen mukaan riski sijoittuu eri numeroille ja esimerkiksi Travellers Business Index:in mukaan riski on sijalla 2. New York Stock Exchange Governance Services ja tietoturvamyyjä Veracode mukaan 80 prosenttia julkisten yhtiöiden hallituksen jäsenistä raportoi keskustelevansa kyberriskeistä jokaisessa tai suurimmassa osista yhtiökokouksista. (Mccollum 2015, 27)

PwC:n Michael Coreyn mukaan organisaation hallituksen jäsenien pitäisi kysyä organisaation johdolta, IT-johdolta sekä sisäiseltä tarkastajalta seuraavat kysymykset: mitkä ovat organisaation riskit? Mitä riskeille tehdään ja tehdäänkö tarpeeksi? Tärkeää on ymmärtää organisaation riskiprofiili ja kuinka paljon kapasiteettia tarvitaan, jotta voidaan hallita niitä riskejä. On myös hyvin tärkeää, että organisaatiossa vallitsee yhteinen kieli, jolla kyberturvallisuus asioista keskustellaan. Hallituksen on ymmärrettävä vastaukset esitettyihin kyberturvallisuutta koskeviin kysymyksiin. Raytheon tutkimuksen mukaan 78 prosenttia tietoturvajohtajista on sitä mieltä, että heidän hallituksensa ei ole saanut perehdytystä kybertuvallisuudesta viimeisen 12 kuukauden aikana. Taas Tripwire tutkimuksen mukaan C-tason johtajista suurissa Yhdysvaltalaisissa

yrityksissä 64 prosenttia oli sitä mieltä, että heidän hallituksensa on niin sanotusti kyberturvallisuus lukutaitoista ja 34 prosenttia sanoi, että heidän hallituksellaan on hyvä ymmärrys tietoturva asioista.

Organisaation eri päättäjät painottavat usein eri asioita kyberturvallisuuteen liittyen ja yleisesti hyväksyttyä kyberturvallisuuskehikkoa ei ole muodostunut. Meltzer suosittelee rakentamaan organisaation oman kyberturvallisuus viitekehyksen, joka auttaa yhteisen kielen löytämisessä kyberturvallisuuteen liittyen. Yhdysvalloissa on muun muassa seuraavanlaisia standardeja, joita on käytetty kyberriskienhallinnassa: U.S. National Institute of Standards and Technology's (NIST's) Cybersecurity Framework, the International Organization for Standardization's ISO 27001 ja ISACA's COBIT. Joitakin aloja säätelevät myös erityislait, joilla on pakottavia vaatimuksia kyberturvallisuuteen liittyen. (Mccollum 2015, 28)

Travis Finstad ja hänen sisäisen tarkastuksen tiimi käyttivät NIST kyberturvallisuus kehikkoa Zions Bancorporationissa ja tekivät koko organisaation kattavan kyberturvallisuus tarkastuksen, jossa pisteyttivät jokaisen viiden valitun kentän yhdestä viiteen asteikolla ja tarkistivat, onko turvallisuuskontrollit toiminnassa ja voisiko jotain kehittää. Tämän jälkeen he puivat tuloksia yhdessä hallituksen, johdon sekä IT-johdon kanssa. Näin saatiin yhteinen ymmärrys kyberturvallisuuden strategiasta ja kontrolleista. Kun kyberriski realisoituu, on tärkeässä asemassa kyky reagoida siihen ja informoida asiakkaita. Tässä korostuukin hyvä riskienhallinta ja valmistautuminen etukäteen sekä kyberriskin ymmärtäminen liiketalousriskinä. Kyberturvallisuuskehikon käyttäminen auttaa myös arvioimaan organisaation sekä tietoturvaosaston suorituskykyä. Koska kyberrikolliset pyrkivät kehittämään jatkuvasti toimintatapojaan, on organisaatioiden pysyttävä tässä kehityksessä perässä, jotta riskeiltä voidaan suojautua. (Mccollum 2015, 29)

Pervez Bamjin mukaan yritykset pitävät kyberriskejä lisääntyvissä määrin osana kokonaisvaltaista riskienhallinnan kehikkoa (ERM), minkä osaksi riski kuuluukin. Sisäiset tarkastajat katsovat kyberriskiä ensin organisaatio tasolta ja tekevät inventoinnin organisaation datasta sekä siitä mikä osa siitä pitää olla suojattuna ja miten se on tällä hetkellä suojattuna. Lisäksi on tärkeää tietää keneltä data pitää olla suojattuna, niin ulkoisilta kuin sisäisiltäkin osapuolilta. Sen jälkeen tarkastetaan teknisiä tietoja, palomuurit sekä datakeskukset ja että kolmansien osapuolien suoja on myös paikallaan. (Mccollum 2015, 30)

Kyberturvallisuus ei onnistu pelkällä IT osaston työllä vaan yhteistyötä vaaditaan niin henkilöstöjohtamisenosaston kuin lakiosastonkin henkilökunnan kanssa. Hyvä vaihtoehto on myös

benchmarkata omaa yhtiötä muihin saman kokoluokan tai saman toimialan yhtiöihin. Yhdysvalloissa finanssialalla ja energia- sekä teknologia-alalla on avointa tiedonjakoa kyberriskeistä ja viimeisistä tietoturvauhkista. Yhdysvaltojen hallitus on myös aikeissa perustaa keskuksia, jonne yritykset voivat jakaa tietoja tietoturva hyökkäyksistä ja jakaa näin tietoa hallitukselle. Tämän tarkoituksena on edistää kyberturvallisuutta kansallisesti. Meltzer ehdottaa myös sotapeli taktiikkaa, jossa tietomurron sattuessa toiseen yhtiöön yhtiöt tekisivät simulaation samasta iskusta tapahtumassa omaan organisaatioonsa. Tämän avulla voitaisiin konkretisoida oman organisaation selviytymistä ja valmiustasoa vastaavanlaista tietomurtoa vastaan. (Mccollum 2015, 30)

Allianz on listannut viisi parasta keinoa vähentää kyberriskejä. 1) Identifioi keskeisien ominaisuuksien riskejä sekä heikkouksia inhimillisenä tekijänä tai yliriippuvuutena kolmansiin osapuoliin. 2) Luo kyberturvallisuus kulttuuri ja aivoriihi tyylinen lähestymistapa riskien hoitamiseen sekä jaa tietoa sidosryhmille. 3) Implementoi kriisiin tai tietomurtoon vastaamissuunnitelma ja testaa sen toimivuutta. 4) Harkitse kuinka fuusiot ja yritysostot sekä muutokset yrityksen rakenteessa vaikuttavat kolmansien osapuolien dataan. 5) Lisäksi tee päätöksiä koskien mitä riskejä vältetään, hyväksytään, kontrolloidaan tai siirretään. Allianz on myös listannut 10 askelta kyberturvallisuuteen. 1) Implementoi tehokas hallinnon rakenne, 2) ylläpidä hallituksen sitoutumista ja valmista oikeanlainen tietoturva, 3) varmista käyttäjien koulutus ja tietoisuus kyberriskeistä, 4) kaikkien verkkojen toimintatapojen seuranta, 5) kybertapahtumien johtamisen menettelytavat, 6) käyttäjien oikeuksien johtaminen ja kontrollointi, 7) turvallisuuskokoonpanon ohjaus, 8) haittaohjelmilta suojautumisen menettelytavat, 9) siirrettävän median kontrollointi sekä 10) matkapuhelimien sekä kotona työskentelyn valvonnan menettelytavat. On arvioitu, että noin 80 prosenttia kyberhyökkäyksistä voisi ehkäistä tai niitä voisi pienentää perus tietoturvan riskienhallinnalla. (Allianz 2015, 13)

Vielä vuonna 2015 on hankaluuksia löytää kyberturvallisuusosaajia. On arvioitu, että maailmanlaajuisesti on 600 000 täyttämätöntä työpaikkaa tietoturva-alalla. ISACA/RSA Conference Security tutkimukseen vastanneet sanovat, että 25 prosenttia tai vähemmän työpaikkaa hakevista ehdokkaista ovat päteviä haettuun tietoturvatyöpaikkaan. Vaihtoehtoina löytää hyvää kyberturvallisuus osaamista on myös ulkoistaa tietoturva osaaminen. Ulkopuolisella on myös usein kokemusta muista yhtiöistä ja näin ollen laajempi näkemys tietoturvauhkista. Iso osa tietoturvan tarkastusprosessista voi olla automatisoitu, mikä tehostaa prosessia. (Mccollum 2015, 31)

Kyberriskien pienentämisessä voidaan käyttää erilaisia strategioita. Kyberrikoksen ehkäisyn strategiana voidaan käyttää muun muassa RAT teoriaa. (The Routine Activity Theory) Tässä teoriassa oletetaan, että rikos ilmenee, kun rikollinen löytää sopivan kohteen, joka on ilman riittävää suojausta. Teoria olettaa, että rikolliset ovat rationaalisia ja tavoittelevat toiminnallaan voittoa. Kyberrikoksen kontekstissa oletuksena on, että 1) kyberrikolliset ovat rikollisesti tai rahallisesti motivoituneita ja 2) etsivät kyberavaruuden tarjoamia mahdollisuuksia kuten anonymiteettiä ja maantieteellistä rajattomuutta sekä hankkivat tarvittavat keinot rikoksen suorittamiseen IT ammattilaisilta. 3) Kohteeksi kyberrikolliset ottavat heikosti suojattuja tietoverkkoja ja käyttävät hyväkseen tilanteita, jossa lainvalvontaviranomaiset ovat estyneitä johtuen lainsäädännöllisistä ja todistusaineistollisista tilanteista erityisesti rajat ylittävissä kyberrikoksissa. On lukemattomia tapoja, joilla rikosteorioita, kuten RAT voidaan hyödyntää kyberriskien pienentämisessä ja kaikilla näillä on tavoitteena 1) lisätä rikollisten vaivannäköä ja ponnistuksia, jotta rikos onnistuisi. 2) Lisätä kiinnijäämisen riskiä ja 3) vähentää rikollisten rikoksesta saamaa palkkiota. (Choo ym. 2011, 725–727)

Käyttäjien tietoisuus varsinkin verkkourkinta tapauksissa on olennaisessa osassa kyberriskien ehkäisyssä. Lisäksi valtion sekä yksityisen sektorin yhteistyö on tärkeässä asemassa. Yhteistyö auttaisi myös siinä, että IT keksinnöt olisivat hyvin ymmärrettyinä myös virkamiehien keskuudessa. Valtio voi myös levittää tietoa kyberrikoksista ja lainvalvontaviranomaisten tutkimuksien tuloksia, esimerkiksi tuotantoyhtiöiden tietojärjestelmien heikkouksista, muidenkin yrityksien tietoon. Näin julkinen ja yksityinen sektori voisivat yhteistyössä kehittää reaaliaikaisen mekanismin, jonka avulla meneillään olevat kyberrikokset voitaisiin ehkäistä reaaliajassa. Näin voitaisiin myös tutkia rajat ylittäviä kyberrikoksia. (Choo ym. 2011, 726)

Kansainvälisten standardien noudattamisella voidaan myös pienentää kyberriskejä. Skopik, Florian & Fiedlerin (2016) mukaan kyberriskejä voitaisiin pienentää ja ehkäistä paremmalla tiedonjaolla. Tänä päivänä tietoa kyberriskeistä jakavat muun muassa ENISA ja CERTs, mutta tiedonjakoa yksityisten yritysten kesken on vähän. Tähän syitä on muun muassa vähäinen laadukas tieto yritykseen kohdistuneista kybertapahtumista sekä pelko maineen menemisestä.

3 RISKIENHALLINTA

3.1 Yleistä riskienhallinnasta

Riskit kuuluvat ja ovat kuuluneet jokapäiväiseen elämään aina. Historiallisina aikoina suurin osa riskeistä, joita ihmiset kohtasivat, olivat fyysisiä ja turvallisuuteen liittyviä. Talouden sekä finanssimarkkinoiden kehityttyä riskit eriytyivät fyysisiin sekä taloudellisiin riskeihin. Sijoittajat voivat siis riskeerata heidän rahansa laittamatta omaa henkeään alttiiksi.

Organisaatioiden riskienhallinnassa on ensimmäisenä tärkeää olla yhteisymmärrys siitä, mikä on riski ja millaisia riskejä organisaatio kohtaa. Huomioitava on yrityksen sisäiset ja ulkoiset toimintaympäristön tekijät, missio sekä strategiset tavoitteet. Riskille ei ole yksiselitteistä määritelmää ja riskin ymmärtäminen on subjektiivista ja riippuu kontekstista. Riski voidaan ymmärtää eri tavalla eri organisaatioissa sekä eri toimialoilla. Vaikka riskille on monta erilaista määritelmää, suurin osa niistä pitää sisällään kuitenkin epävarmuuden sekä tappion vaaran. Riskin käsitteen voidaan nähdä myös sisältävän mahdollisuuden voittoon. (Hardy, Karen, Runnels & Allen 2015, 33)

Riski ja mahdollisuus kulkevat käsi kädessä. Tapahtumalla voi näin ollen olla niin negatiivinen kuin positiivinenkin vaikutus tai molemmat. Tapahtumat, joilla on negatiivinen vaikutus edustavat riskiä, joka voi esimerkiksi ehkäistä arvonluontia. Taas tapahtumat joilla on positiivinen vaikutus voivat syrjäyttää negatiivisen vaikutuksen tai ne voivat edustaa mahdollisuuksia. Mahdollisuudet tarkoittavat sitä tilannetta, että tapahtuma tapahtuu ja se vaikuttaa positiivisesti yrityksen toimintaan. (COSO 2004, 8)

Riskienluokittelu kuuluu riskienhallinnan perusteisiin. Riskien luokittelulla riskit saadaan yhteismitallisimmiksi ja näin niiden keskenään vertailusta tulee helpompaa. Lisäksi näin voidaan lisätä ymmärrystä eri riskien keskinäisistä suhteista. Riskit voidaan jakaa neljään riskilajiin: 1) strategiset riskit, 2) operatiiviset riskit, 3) taloudelliset riskit ja 4) vahinkoriskit. *Strategiset riskit* liittyvät organisaation pitkän aikavälin strategisten tavoitteiden saavuttamiseen. Strategiset riskit voidaan jakaa vielä ulkoisiin ja sisäisiin strategisiin riskeihin. Ulkoiset strategiset riskit voivat liittyä yrityksen toimintaympäristön muutoksiin sekä kilpailijoihin. Sisäiset strategiset riskit taas voivat liittyä esimerkiksi strategian toimeenpanon epäonnistumiseen. *Operatiiviset riskit* liittyvät yrityksen jokapäiväisiin toimintoihin ja ovat välittömiä tai välillisiä vahinkojen tai maineen riskejä. Nämä riskit voivat seurata esimerkiksi henkilöstöstä tai epäonnistuneista sisäisistä prosesseista. Merkittävimpinä operatiivisina riskeinä voidaan pitää liiketoiminnan

keskeytysriskiä. Sopimus- ja vastuuriskit ovat myös osa operatiivisia riskejä. *Taloudelliset riskit* taas liittyvät yrityksen rahaprosessia uhkaaviin riskeihin. Esimerkiksi yrityksen velalliset eivät kykene maksusuorituksiin, mikä vaikuttaa yrityksen maksuvalmiuteen. *Vahinkoriskit* käsittävät työkykyyn sekä työtapaturmiin liittyvät riskit. Myös ympäristöön liittyvät riskit kuten saastumisriski kuuluvat vahinkoriskeihin. (Ilmonen, Kallio, Koskinen & Rajamäki 2010, 64–69)

Riskejä voidaan luokitella myös muillakin perusteilla, kuten vakuutettavat ja ei-vakuutettavat riskit tai välittömät ja välilliset riskit. Vakuutettavista riskeistä synonyymina pidetään usein vahinkoriskejä ja ei-vakuuttettavien synonyymina taas liikeriskejä. Liikeriskeissä on myös voiton mahdollisuus, mitä vahinkoriskeissä taas ei ole. (Ilmonen ym. 2010, 69) Riski voidaan jakaa edelleen osa-alueisiin. Riskin osa-alueet ovat 1) lähde, 2) tapahtuma, 3) seuraus, 4) syy 5) kontrolli ja 6) aika ja paikka. *Lähde* tarkoittaa tekijää, jolla on mahdollisuus aiheuttaa vahinkoa esimerkiksi yrityksen kilpailijat. *Tapahtuma* taas tarkoittaa asiaa, joka on tapahtunut siten että riskin lähde alkaa vaikuttamaa organisaation toimintaan tai ajankohta jolloin riskin mittari tai muu indikaattori saavuttaa tietyn tason. *Seuraus* on tulos tai vaikutus organisaation sidosryhmiin tai voimavaroihin. Riskin *syy* tarkoittaa mitä ja miksi jotakin on tapahtunut. *Kontrollilla* tarkoitetaan esimerkiksi yrityksen turvallisuusjärjestelmiä eli yleisesti riskienhallintaa ja sen eri tasoja. *Aika ja paikka* kuvaavat milloin tapahtuma on sattunut. (AZ/NZS 436:2004, 38)

Riskienhallintaan on olemassa monia erilaisia standardeja kuten COSO, ISO 31000, FERMA ja AZ/NZS. ISO 31000 standardia voidaan pitää päivitettynä versiona AZ/NZ standardista. (Ilmonen ym. 2010, 28) Riskienhallinnassa on tiettyjä perusperiaatteita. Riskienhallinta on keskeinen osa strategista johtamista kaikissa organisaatioissa. Onnistuneen riskienhallinnan pitäisi olla oikeassa suhteessa organisaation riskitason kanssa ja linjassa muiden yritysten toimien kanssa sekä sen on oltava osa rutiininomaisia toimia ja samalla dynaaminen vastaamalla muuttuviin olosuhteisiin. Riskienhallinnan fokus on merkittävien riskien arvioinnissa sekä sopivien riskeihin reagoimiskeinojen implementoinnissa. Riskienhallinta parantaa mahdollisten sekä hyvien että haittatekijöiden vaikutusten ymmärtämistä organisaatioon. Se parantaa menestyksen todennäköisyyttä ja vähentää organisaation tavoitteiden saavuttamisen epävarmuutta. (www.ferma.eu) Riskienhallinnan pitäisi olla jatkuva prosessi, joka tukee organisaation strategiaa. Kaikissa uusissa hankkeissa on mahdollisuus saada hyötyä, mutta myös tappioita ja näin ollen lisääntyy epävarmuuden aste.

3.2 Riskien arviointi

Riskienhallinnassa on myös arvioitava riskien tasoja. Riskien tasojen arvioinnissa voi hyödyntää riskimatriisia, jonka vertikaaliakselilla on riskien todennäköisyys ja horisontaaliakselilla taas riskien vakavuus. Riskejä arvioitaessa on mietittävä, onko riski siedettävällä tasolla vai onko ryhdyttävä toimenpiteisiin. Riski voidaan näin jakaa viiteen joukkoon sen todennäköisyyden sekä seurauksen perusteella. Seuraus voi olla joko 1) merkityksetön, 2) pieni, 3) keskiverto, 4) suuri tai 5) todella suuri. Taas todennäköisyys riskissä voi olla 1) melkein varma, 2) todennäköinen 3) mahdollinen, 4) epätodennäköinen ja 5) harvinainen. Matriisista nähdään riskin seurauksen ja todennäköisyyden perusteella onko riski matala, keskisuuri, korkea vai todella suuri. (Risk management handbook, 28)

Eritasoiset riskit vaativat erilaisia riskienhallinnan toimenpiteitä. Esimerkiksi punaisella merkityt riskit ovat sietämättömiä, riippumatta siitä millaisia etuja se saattaisi tuoda, ja riskin pienentämisen toimenpiteet ovat välttämättömiä niiden kustannuksista riippumatta. Riskit vaativat välitöntä reagointia. Kun riski on sietämättömällä tasolla, on oletuksena, että riskiä pienennetään, elleivät kustannukset ole todella suhteettomia saatuun hyötyyn nähden. Oranssin alueen riskit eli korkeat riskit vaativat myös oikeanmukaista arviointia sekä huomiota. Korkeasta riskistä on raportoitava ylimmälle johdolle ja toimenpiteitä riskin pienentämiseksi on tehtävä. Keskijoukossa tai niin sanotulla keltaisella alueella olevien riskien mahdolliset hyödyt sekä haitat on otettu huomioon ja mahdollisuudet tasapainotettu mahdollisia tappioita vastaan. Tämän tasoisten riskien valvonta suoritetaan normaaleissa liiketoiminnan käytänteissä. Matalimmassa joukossa eli vihreällä merkityt riskit ovat toiminnalle merkityksettömiä tai ne ovat niin pieniä, että toimenpiteitä ei välttämättä tarvita. (Risk management handbook, 28)

Kun riski on taas lähellä merkityksetöntä tasoa, silloin toimenpiteisiin on ryhdyttävä vain, jos hyödyt ylittävät riskin pienentämisen kustannukset. Kaikki riskit eivät siis vaadi samantasoisia toimenpiteitä tai seurantaa. Yritysten onkin tehtävä säännöllisin väliajoin kartoitusta sekä arvioita kohtaamistaan riskeistä, jotta riskienhallinta pysyy ajan tasalla. (AZ/NZS 436:2004, 55)

Seuraus Todennäköisyys	1 Merkityksetön	2 Pieni	3 Keskiverto	4 Suuri	5 Todella suuri
Melkein varma	Keskisuuri riski	Keskisuuri riski	Korkea riski	Todella suuri	Todella suuri
Todennäköinen	Matala riski	Keskisuuri riski	Korkea riski	Korkea riski	Todella suuri
Mahdollinen	Matala riski	Keskisuuri riski	Keskisuuri riski	Korkea riski	Korkea riski
Epätodennäköinen	Matala riski	Matala riski	Keskisuuri riski	Keskisuuri riski	Korkea riski
Harvinainen	Matala riski	Matala riski	Matala riski	Matala riski	Keskisuuri riski

Kuvio 3. Riskimatriisi. Riskimatriisilla voidaan arvioida riskejä niiden seurauksen sekä todennäköisyyden perusteella.

Riskienhallinta toimenpiteet voidaan jaotella riskin siirtämiseen sekä yrityksen omiin riskienhallinta toimenpiteisiin. Riskit voidaan siirtää toisen osapuolen kannettaviksi vakuutuksilla, sopimuksilla tai rahoitusratkaisuilla. Sopimuksella siirtäminen voi tarkoittaa esimerkiksi toimintojen ulkoistamista. Riskin vakuuttamisessa yritys siirtää riskin aiheuttaman tappion osittain vakuutusyhtiön kannettavaksi. Yrityksen omia riskienhallinnan toimenpiteitä eli riskin kontrollointia ovat 1) riskin hyväksyminen, 2) riskin pienentäminen sekä 3) poistaminen ja välttäminen. Riskien hyväksyminen on kannattavaa yleensä pienten ja epätodennäköisten riskien osalta. Riskien pienentäminen tarkoittaa riskin todennäköisyyden tai vaikutuksen pienentämistä ja se voidaan toteuttaa taas lisäämällä esimerkiksi henkilöstöresursseja ja suojelutoimenpiteitä. Nollatoleranssi riskit eli riskit, jotka ovat poistettava, ovat yleensä turvallisuus- sekä henkilöriskeihin liittyviä. Täysin poistettavia riskejä on olemassa kuitenkin verrattain vähän. (Ilmonen ym. 2010, 116–121)

IT-riskien eli tietoturvariskien hallinnassa on tiettyjä rajoitteita, jotka on huomioitava. 1) Poliittiset rajoitukset, viranomaiset tai lainsäädäntö voivat rajoittaa tehokkaimpien riskienhallintakeinojen käyttöä, jos ne uhkaavat yhteiskunnassa arvostettuja arvoja. Tästä esimerkkinä toimii tietosuojalainsäädäntö, joka suojelee henkilöiden yksityisyyttä ja näin estää yrityksiä saamasta kaikkea tarpeellista tietoa esimerkiksi uudesta työntekijästä suojautuakseen väärinkäytösriskeiltä. 2) Strategiset rajoitteet tulevat yrityksen tavasta toteuttaa strategiaa. Jos strategiassa on päädytty ostamaan IT-palvelut, riskienhallintakeinojen tulee olla myös kumppaneiden hyväksymiä. 3) Alueelliset rajoitteet koskevat maantieteellisesti hajautuneita yrityksiä, mikä rajoittaa manuaalisten korjaustoimenpiteiden käyttömahdollisuuksia. 4) Taloudellisen tilanteen

rajoitteet tarkoittavat yleisen taloudellisen tilanteen heikkoutta, mikä voi johtaa siihen, että riskienhallinnassa on keskityttävä enemmän muiden riskilajien hallintaan kuten markkinariskien hallintaan. 5) Menetelmälliset rajoitteet, IT-riskien systemaattista hallintatyötä helpottaa IT-osaston muu systemaattinen toiminta. Jos niitä ei kuitenkaan ole joudutaan systematiikkaa luomaan. 6) Henkilöstöön ja kulttuuriin liittyvät rajoitteet on otettava huomioon, koska eri ihmisillä on erilainen käsitys tietohallinnosta ja siihen liittyvistä asioita. Kulttuurillisten rajoitteiden tunnistamisen jälkeen on helpompaa muodostaa tietojärjestelmistä yhteistä käsitystä. (Ilmonen ym. 2010, 116–122)

3.3 Kokonaisvaltainen riskienhallinta

Enterprise risk management (ERM) eli yrityksen kokonaisvaltainen riskienhallinta, on riskienhallintaa, jossa yrityksen kohtaamia riskejä tarkastellaan kokonaisuutena. Kokonaisvaltainen riskienhallinta on prosessi, johon vaikuttavat yhtiön hallitus, johto sekä muut työntekijät. Sitä toteutetaan koko organisaation strategia- sekä suunnitteluprosessissa ja se on suunniteltu tunnistamaan tekijöitä jotka voivat vaikuttaa yhtiöön sekä hallitsemaan riskejä riskinottohalun piirissä. Näin varmistetaan se, että yhtiön tavoitteiden saavuttaminen olisi riittävällä pohjalla. Kokonaisvaltaisessa riskienhallinnassa on laajasti tukeuduttu COSO ERM- standardiin, joka jakautuu viitekehykseen sekä menetelmiin. (COSO 2004, 2)

Kokonaisvaltaisen riskienhallinnan viitekehys perustuu kokonaisvaltaisen riskienhallinnan määritelmään. Viitekehyksessä kuvataan käsitteet ja periaatteet joiden avulla johto voi arvioida sekä kehittää riskienhallintaa ja näin ollen viitekehys määrittelee yrityksen riskienhallinnan. (Ilmonen ym. 2010, 28) Viitekehys on muodostettu saavuttamaan yrityksen toiminnalliset tavoitteet, jotka on luokiteltu neljään ryhmään. 1) Strategia: korkean tason tavoitteet, jotka ovat linjattu tukemaan missiota. 2) Operaatiot: tehokasta resurssien käyttöä. 3) Raportointi. 4) Vaatimustenmukaisuus eli lainsäädännön noudattaminen. Kokonaisuuden osa-alueiden kategorisointi auttaa keskittymään tiettyihin erillisiin kokonaisvaltaisen riskienhallinnan tavoitteisiin. Nämä luokat ovat erillisiä, mutta osittain päällekkäisiä ja tietty tavoite voi kuulua useampaankin luokkaan. Yrityksen toiminnalliset tavoitteet on esitetty vertikaalisilla sarakkeilla. (COSO 2004, 11)

Kokonaisvaltainen riskienhallinta koostuu kahdeksasta toisiinsa yhteydessä olevista osatekijöistä, jotka on integroitu johtamisprosessiin. Nämä osa-alueet ovat esitetty horisontaalisilla riveillä. Ja näitä ovat 1) sisäinen ympäristö, 2) tavoitteen asettelu, 3) tapahtumien tunnistaminen 4) riskien arviointi, 5) riskeihin vastaaminen, 6) valvonta toimenpiteet, 7) tieto & viestintä ja 8) seuranta. Viimeinen osio huomioi yrityksen yksiköt eli tytäryhtiöt, toimialayksiköt sekä liiketoimintayksiköt ja näin ollen käsittää koko organisaation. (COSO 2004, 11)

Kuvio 4. COSO ERM viitekehys (www.riskikompassi.fi)

4 KYBERVAKUUTUS

4.1 Kybervakuutuksen kehitys

Vakuutustoimintaa voidaan kuvata seuraavanlaisesti:

”Tietyn riskinalaiset yksiköt, vakuutuksenottajat, sopivat vahinkojen tasaamiseen erikoistuneen laitoksen, vakuutuslaitoksen eli vakuutuksenantajan kanssa siitä, että riskin toteutuessa vakuu-

tuksenantaja korvaa siitä aiheutuneen vahingon. Korvauksensaantioikeuden vastikkeeksi vakuutuksenottajat suorittavat vakuutusmaksun vakuutuksensaajalle.”(Rantala & Kivisaari 2014, 70)

Vakuutuksenottajan ja – antajan välistä oikeussuhdetta kutsutaan vakuutukseksi. Vakuutuksen ominaisuuksia ovat 1) sattumanvaraisuus, 2) vahingon mahdollisuus 3) vakuutusmaksun ja riskin vastaavuus 4) tasaus suuren joukon kesken sekä 5) vakuutuksenantajan tulee olla vakuutuksenottajasta erillinen subjekti. (Rantala & Kivisaari 2014, 70)

Kaikkia riskejä ei ole mahdollista vakuuttaa. Riskin vakuutuskelpoisuus muodostuu tietyistä edellytyksistä, jotka muodostavat vakuutuskelpoisuuden käsitteen. 1) riskin on oltava ennustettavissa ja 2) riskin on oltava edunsaajasta riippumaton. Tämä ehto on yleensä syynä siihen, ettei liikeriskejä voida vakuuttaa. Jos vakuutus korvaisi kaikki mahdolliset vahingot, johto voisi ryhtyä uhkarohkeisiin toimiin. 3) riskin on myös oltava ajallisesti stabiili eli riski ei saa ajan myötä muuttua ennalta arvaamattomasti suuria määriä sekä 4) riskin toteutumisen on oltava harvinainen. Jos riski on kovin yleinen saattaa vakuutusmaksu muodostua matemaattisesti laskettuna jopa suoritettavan korvauksen suuruiseksi. (Rantala & Kivisaari 2014, 79–80)

Kybervakuutus on vakuutus, joka kattaa kyberhyökkäyksistä organisaatioille aiheutuneita kuluja ja auttaa näin organisaation toipumista hyökkäyksestä. Kybervakuutuksessa on kaksi liiketoiminnan näkökulmaa. Ensinäkin vakuutuksenantajat haluavat saada kybervakuutusmaksuista tarpeeksi tuottoja, jotta ne ylittävät kyberrikoksista aiheutuneet tappiot pitkällä aikavälillä. Toiseksi vakuutuksenottajat haluavat siirtää riskiä kybervakuutuksen avulla ja näin maksimoida hyödyn. Vakuutusyhtiölle kybervakuutus edustaa kasvumahdollisuutta, koska kyberriskeiltä suojautumisen tarve on jatkuvasti lisääntyvä. Vakuuttajien on onnistuttava hinnoittelemaan kybervakuutus oikein, jotta se myy markkinoilla ja lisäksi tehtävä tämä kilpailijoita paremmin. (Majuca, Yurcik & Kesan 2005, 2)

Bienerin ym. (2015, 135) mukaan kybervakuutusmarkkinoille on tyypillistä tuotteen korvaussuojan sekä muiden ominaisuuksien muuttuminen nopeaan tahtiin kilpailijoiden keskuudessa. Tuote vaatii kyberriskien luonteen takia erikoistumista vakuutusehtojen kirjoittamisessa, koska riski näyttäytyy uniikkina erilaisille yhtiöille niiden toimialasta riippuen. Se, kuinka iso yritys on sekä miten se on tallentanut asiakastietonsa, vaikuttaa paljon vakuutusehtojen kirjoittamiseen. Lainsäädännölliset rajoitukset voivat ehkäistä tietyntyyppisiä vakuutusehtoja. Muun muassa monissa maissa sakkoja vastaan vakuuttaminen on kiellettyä. Lainsäädännön muutokset ovatkin vakuutusyhtiöille riski.

Vakuutettavuuden kriteeri	**Pää löydökset**	**Arviointi**
Satunnaisuus tapahtumien esiintymisessä	-Tiedon puute -Kyberriskien muuttuva luonne -Riskipoolit ovat vielä liian pieniä -Riittävän jälleenvakuuttamisen puute	Ongelmallinen
Maksimaallinen mahdollinen vahinko	-Maksimaalinen vahinko kyberriskeissä on pienempi kuin muissa operatiivisissa riskeissä -Vakuutusyhtiöt suojautuvat maksimivahinkoja vastaan korvausrajoilla	Ei ongelmallinen
Keskimääräinen tappio tapahtumasta	-Keskimääräinen tappio on pienempi kuin muilla operationaalisilla riskeillä -Riippuu yrityksen koosta, suojautumisen tasosta sekä institutionaalisesta sitoutumisesta tietoturvaan	Ei ongelmallinen
Riskille altistuminen	-Lisääntyvissä määrin kyberhyökkäyksiä -Riippuu kybertapahtumien kategorisoinnista (esim. inhimilliset tekijät dominoivat muita kategorioita)	Ei ongelmallinen
Epäsymmetrinen informaatio	-Moraalikato sekä haitallinen valikoituminen sisältää suuren teoreettisen uhkan: omavastuut auttavat vähentämään moraalikatoa -Etukäteen tehty riskiarviointi ja ISO sertifikaatit auttavat taas vähentämään haitallista valikoitumista	Ongelmallinen
Vakuutusmaksu	-Korkeat vakuutusmaksut ja muut kulut johtuen suurista epävarmuuksista -Vakuutusehdoissa suuria eroja toimialojen välillä -Toistaiseksi vähän kilpailijoita (odotetaan lisääntyvän tulevaisuudessa) -Lisäkustannuksia esim. etukäteinen riskiarviointi	Kasvavissa määrin vähemmän ongelmallinen
Korvausrajat	-Vakuutus korvaa yleensä max US $ 50 miljoonaa -Paljon ei korvattavia kuten itseaiheutettu vahinko, terrorismi jne. -Epäsuoria kustannuksia kuten maineen menetys ei voi mitata eikä yleensä korvata -Tuotteen monimutkaisuus voi olla myös ongelmallinen mm. riskin dynaaminen luonne	Ongelmallinen
Julkiset politiikat	Vakuutuspetos voi olla houkutteleva, koska hakkerointia on vaikea havaita ja jäljittää	Vähemmän ongelmallinen
Lainsäädännölliset rajoitteet	-Monissa maissa laitonta vakuuttaa sakkoja vastaan -Lainsäädännön muuttumisen riski -Arkaluonteisen tiedon paljastumisen riski	Vähemmän ongelmallinen

Kuvio 5. Kyberriskien vakuutettavuuden arviointia. (Biener ym. 2015)

Biener ym. (2015, 148) ovat tutkimuksessaan arvioineet kybervakuutuksen vakuutettavuutta. Yllä olevassa taulukossa he listaavat vakuutettavuuden kriteereiksi seuraavat elementit: satunnaisuus tapahtumien esiintymisessä, maksimaalinen mahdollinen vahinko, keskimääräinen tappio tapahtumasta, riskille altistuminen, epäsymmetrinen informaatio, vakuutusmaksu, korvausrajat, julkiset politiikat ja lainsäädännölliset rajoitteet. Ongelmallisina nähdään satunnaisuus tapahtumien esiintymisessä, epäsymmetrinen informaatio sekä korvausrajat. Riskistä on vielä liian vähän tietoa ja riskipoolit ovat vielä pieniä. Lisäksi riski on jatkuvasti muuttuva ja jälleenvakuuttaminen ei ole vielä riittävällä tasolla. Epäsymmetrinen informaation nähdään myös ongelmallisena, vaikkakin haitallista valikoitumista ja moraalikatoa pystytään hallitsemaan jossain määrin muun muassa vakuutusehdoilla sekä etukäteen tehdyillä riskiarvioinneilla. Korvausrajoissa taas ongelmana nähdään kybertapahtumista aiheutuvat vahingot, joita ei suoraan pystytä korvaamaan, kuten muun muassa maineen menetys. Vähemmän ongelmallisina nähdään vakuutusmaksu, julkiset politiikat sekä lainsäädännölliset rajoitteet. Ongelmattomina taas pidetään kyberriskien vakuuttamisen kannalta maksimaalista mahdollista vahinkoa, keskimääräistä tappiota tapahtumasta sekä riskille altistumista.

Kybervakuutus on kehittynyt alun perin tavallisesta vastuuvakuutuksesta. Paljon erimielisyyksiä on ollut vakuutusyhtiöiden sekä yritysten välillä siitä, mikä on aineellista omaisuutta sekä mikä on aineellinen vahinko, koska kyberriskien toteutuminen ei yleensä vahingoita fyysistä omaisuutta eikä näin aiheuta fyysistä vahinkoa yhtiölle. Tuomioistuimet eri puolilla Yhdysvaltoja ovat vuosien saatossa olleet eri mieltä siitä, mikä on aineellista omaisuutta. Vuonna 1997 Florida District Court määräsi, että elektroniset sarjanumerot, henkilötunnukset sekä puhelinnumerot eivät ole fyysistä omaisuutta. (Majuca ym. 2005, 4)

Ensimmäinen tietojärjestelmien hakkerointiin liittyvä vakuutus tuli markkinoille 1998. Teknologia yhtiöt tekivät yhteistyötä vakuutusyhtiöiden kanssa tarjoten teknologiapalveluita sekä ensimmäisen osapuolen vakuutusturvaa. International Computer Security Association (ICSA) tarjosi ensimmäisenä hakkerointiin liittyvää vakuutusta vakuutena palveluidensa luotettavuudesta ainoastaan 250 000 dollarin maksimi vakuutuskorvaus määrällä vuodessa. Hakkerointiin liittyvät ensimmäiset yksinkertaiset vakuutukset kehittyivät näin hyvin pienistä korvaussummista,

jotka kattoivat vain ensimmäisen osapuolen suojan, suurempiin korvaussummiin ja kyberhyökkäyksistä aiheutuvien tappioiden korvaaviin monimutkaisempiin vakuutuksiin. Cigna Corp, Cisco Systems ja NetSolve toivat myös markkinoille vuonna 1998 vakuutuksen hakkerointia sekä toiminnan keskeytymistä kattamaan. Tämä vakuutus kattoi myöskin ensimmäisen osapuolen riskit ja vakuutussuoja oli maksimissaan 10 miljoonaa dollaria vuodessa. Vielä samana vuonna myös J.S. Wurzler Underwriting, IBM ja Sedgwick toivat markkinoille vastaavanlaisen vakuutuksen. Vuonna 2000 Counterpane ja Lloyd's of London sekä myös Marsh McLennan yhteistyössä AT&T kanssa vuonna 2001 lanseerasivat vastaavanlaisen vakuutuksen. (Majuca ym. 2005, 4) Vakuutusmeklareilla oli kuitenkin vaikeutuksia saada tuotetta myytyä yrityksille ja saada ostajat vakuuttumaan sen hyödyllisyydestä ja vain harvat yritykset ostivat sen. (Voelker 2015, 42–44)

Vakuutusyhtiö AIG oli ensimmäinen, joka toi markkinoille vakuutuksen mikä kattoi myös kolmannen osapuolen vahinkoja vuonna 2001. Tämä oli alku entistä kattavammille tietojärjestelmien hakkerointiin liittyville vakuutuksille ja tämän tuotteen suurin korvaussuoja oli 25 miljoonaa dollaria vuodessa. Lisääntynyt riski sekä lainsäädännön noudattaminen olivat syitä kybervakuutuksen kehitykseen. Vuonna 2001 syyskuun 11. päivä riskin havaitseminen muuttui dramaattisesti, kun kolme vakavinta internet virushyökkäystä tapahtui kolmen kuukauden aikavälillä. Code Red heinäkuussa, Nimda syyskuussa ja Klez lokakuussa 2001. Aikaisemmin myös vuonna 2000 helmikuussa tapahtui sarja palvelunestohyökkäyksiä, jotka kohdistuivat merkittäviä Yhdysvaltalaisia yhtiöitä kohtaan. Hyökkäykset estivät viiden suosituimman nettisivun toimimisen ja lisäksi hidastivat koko internetiä. Hyökkäykset ovat kohdistuneet yritysten lisäksi valtion toimistoihin kuten Yhdysvaltojen senaattiin, Federal Bureau of Investigation (FBI), National Aeronautics and Space Administration (NASA) sekä Department of Defense (DoD). Virus nimeltä Love Bug vuonna 2000 vaikutti 20 maahan sekä 45 miljoonaan käyttäjään aiheuttaen arviolta 8,75 biljoonan dollarin tappiot. Vuosien 2000 ja 2003 välillä internettiin liittyvä riski on näin ollen noussut merkittävästi, johtaen yksilöiden sekä organisaatioiden tarpeeseen hallita sitä. Lisääntynyt riski ja lainsäädännön noudattaminen ovat ensisijaisia syitä, jotka vaikuttivat kybervakuutuksen kehitykseen. (Majuca ym. 2005, 6)

Nykyajan kybervakuutukset ovat pitkälle jalostuneita ja tarjoavat ensimmäisiin vakuutuksiin verrattuna myös kolmannen osapuolen suojaa sekä korkeammat korvausrajat. Toinen huomattava piirre kehittyneimmissä kybervakuutuksissa on niiden kapeat korvauspiirit, jotka on suunniteltu houkuttelemaan erilaisia tarpeita omaavia asiakkaita. Kapeasti määritellyt korvaustapah-

tumat mahdollistavat sen, että vakuutusyhtiöt voivat sulkea ennakoimattomia tapahtumia korvauspiirin ulkopuolelle. Lisäksi, kun korvauspiiri on määritelty erityisesti, vakuuttajat voivat erikoistua markkinoilla ja tarjota tuotteitaan tietyille markkinoille ja asiakkaille. Esimerkiksi asiakkaille, jotka haluavat suojaa vain omien prosessien vaurioitumiselta, tai asiakkaille jotka haluavat vakuutussuojaa vain kolmannen osapuolen vastuun varalle, on suunniteltu erilaiset kybervakuutustuotteet. Kybervakuutuksien kehityksessä on näin ollen siirrytty tuotteiden sekä asiakkaiden segmentointiin. (Majuca ym. 2005, 7)

Majucan ym. (2005, 7) mukaan kybervakuutukseen niin kuin muihinkin vakuutustuotteisiin liittyy haitallinen valikoituminen sekä moraalikadon ongelmat. Haitalliseen valikoitumiseen vastatakseen vakuutusyhtiöiden täytyy suorittaa yrityksen läpi yksityiskohtainen riskiarviointi. Ehtona vakuutuksen saamiselle on riskiarvioinnin tekeminen, jossa vakuutusyhtiö arvioi ja käy läpi lukemattomia yrityksen prosesseja saadakseen selvyyden yrityksen haavoittuvuudesta. Haitallinen valikoituminen on mukana myös kybervakuutuksissa. Yritykset, jotka ovat kärsineet kyberhyökkäyksistä aikaisemmin ostavat kybervakuutuksen todennäköisemmin kuin ne yritykset, jotka eivät ole kärsineet hyökkäyksistä aikaisemmin. Lisäksi yritykset, joilla on korkea riski kyberhyökkäyksiin ostavat todennäköisemmin vakuutuksen. Vakuutusyhtiöt kamppailevat näiden epävarmuuksien kanssa vakuutusmaksulaskelmissaan jatkuvasti ja vaativat siksi yrityksiltä paljon tietoja tietoturvatasosta sekä virtuaalisista laitteista.

Vakuutettujen yritysten käytös kyberriskejä kohtaan saattaa myös muuttua vakuutuksen oton jälkeen. Tätä voidaan hallita rahallisilla kannustimilla kuten alennuksilla yrityksille, jotka parantavat kyberturvallisuuttaan. Yrityksien luottaminen pelkästään kybervakuutukseen kyberriskien hallintakeinona on riittämätön vastaus kasvavaan ongelmaan. Yrityksien on jatkuvasti parannettava valmiuksiaan tunnistaa ja havaita tietomurtoja, paikata ohjelmistojen tietosuoja-aukkoja yhä nopeammin sekä eristää elintärkeitä järjestelmiä ja tietoja. Yritykset, joilla on tietoturvajohtaja (Chief Information Security Officer, CISO) on raportoitu kärsineen pienemmistä tappioista, kun kyberhyökkäys on tapahtunut kuin yritysten, joilla ei ole erillistä tietoturvajohtajaa. (Shackelford 2012, 354)

4.2 Kybervakuutuksen ostoon vaikuttavat tekijät

Kyberturvallisuuden johtaminen on kohdannut monia haasteita ja haasteita on aiheutunut myös kybervakuutuksien suunnittelijoillekin. Ensinäkin yksittäiset firmat, jotka hakevat suojaa kriittisiä tietoja varten muodostavat korreloituneen riskin käyttämiensä teknologioiden kautta. Tietotekniikka infrastruktuuria dominoi lisäksi muutamat keskeiset teknologiat, jolloin yritykset ovat samalla tavoin haavoittuvia ja näin riski korreloituu. Toiseksi, kun riski lopulta toteutuu ja tapahtuu tietomurto, on yritysten vaikea todistaa aiheutunut tappio vakuutusyhtiölle ja näin ollen on vakuutusyhtiöiden vaikea määrittää korvaussummaa, joka vastaisi aiheutunutta tappiota. Suurin osa tappiosta on myös aineetonta, kuten maineen menetys. Yhtiöillä on usein myös vaikeuksia havaita tunkeilijoita järjestelmissään ja kaikki nämä johtavat siihen, että yritykset harvoin saavat korvausta kaikista kärsimistään tappioista. Tutkimuksen mukaan on 68 prosentin todennäköisyys havaita suuri tietomurto eli murto, joka koskee yli 10 000 henkilötietoja ja 51 prosentin todennäköisyys havaita pieni tietomurto, jolloin 100 henkilötietoa tai vähemmän on varastettu. Kolmanneksi vakuutusyhtiöiden on vaikea havaita yhtiöiden tietosuojan taso. Yhtiöt eivät yleensä paljasta tietosuojansa tasoja, jotta tieto ei leviä ulkopuolisille ja mahdollisesti hakkereiden käsiin. (Hulisi, Srinivasan & Nirup 2011, 497)

Gordon & Loeb (2002) mukaan, kun tietosuojan haavoittuvuus nousee kynnystason yli, yritysten tietosuojaan käyttämien varojen harkinta vähentää tietosuojaan sijoittamista. Kyberriskien korrelaatiosta aiheutuvia vaikutuksia voidaan myös pienentää yritysten tietoturvaan liittyvällä tiedonjaolla. Heidän mukaan yritykset vähentävät investoimista tietoturvaan, ellei oikeanlaisia kannustimia ole. Hulisi ym. (2011, 497) täydentää, että yritykset eivät voi täydellisesti todistaa tietomurrosta aiheutuvia tappiota vakuutusyhtiöille sekä vakuutusyhtiöiden on vaikea määritellä ja tarkastaa yhtiöiden itse omaan tietoturvaan käyttämiä panoksia. Nämä tekijät vaikuttavat yritysten riskienhallinta strategioihin koskien kyberturvallisuutta.

Hulisi ym. (2011, 508) mukaan yritykset investoivat vähemmän tietosuojaan sekä kybervakuutukseen kuin yhteiskunnallisesti optimaalinen taso olisi, kun kyky tappion täydelliseen todistamiseen on epätäydellinen ja kun riski on korreloituva. Se, että yritykset investoisivat yhteiskunnallisesti optimaalisen tason verran vakuutukseen sekä tietosuojaan, riippuu siitä, kuinka ne voivat todistaa oman tietosuojatasonsa. Jos itsesuojelu on havaittavissa niin, että vakuutus on mahdollista tehdä tietosuojatason mukaisesti, niin tällöin tietosuoja ja vakuutus käyttäytyvät toistensa komplementteina. Tällaisissa tapauksissa valtio voi houkutella yhtiöitä valitsemaan yhteiskunnallisesti optimaalisen tietosuojatason tarjoamalla tukea tietosuojaan. Mutta jos tietosuojaa ei voida havaita ja näin ollen vakuutussopimus perustuu vain vakuutuksen korvauspii-

riin, silloin tietosuoja ja vakuutus toimivat toistensa substituutteina ja yritykset ostavat enemmän vakuutuksia kuin yhteiskunnalliset optimaalista olisi ja sijoittavat vähemmän tietosuojaan kuin yhteiskunnallisesti optimaalinen taso olisi. Tällaisissa tapauksissa taas valtion pitäisi verottaa vakuutusmaksuja, jotta saavutettaisiin haluttu tulos. Tutkimuksen tulos on pätevä riippumatta siitä, ovatko vakuutusmarkkinat täydelliset vai ei, joten uudistamalla tällä hetkellä epätäydellisiä vakuutusmarkkinoita ei saataisi tehokasta tulosta kyberturvallisuuden riskienhallintaan.

Betterleyn (2015, 8) mukaan aikaisemmin ennen kyberhyökkäyksen toteutumista vakuutusyhtiöiltä saatavalla tietoturvallisuuteen liittyvällä ohjauksella ei ollut vaikutusta kybervakuutuksen ostoon. Nykyään tilanne on kuitenkin toinen ja trendinä on, että ennakoiva ohjaus tietoturvallisuuteen toimii yhtenä tekijänä, jonka perusteella yritykset ostavat kybervakuutuksen. Nämä palvelut toimivat myös kilpailutekijänä vakuutusyhtiöiden kesken.

March LCC mukaan vain yhdellä kolmasosalla yrityksistä on kybervakuutus ja vuoden 2013 aikana niiden myynti pankeille, sairaaloille, jälleenmyyjille sekä muille yrityksille nousi 20 prosenttia. Ponemon Instituten mukaan monet yritykset sanovat ostavansa kybervakuutuksen tulevaisuudessa, mutta lähes yhtä monet sanovat, etteivät osta kybervakuutusta sen korkean hinnan sekä vakuutusehdoissa olevien rajoitusten ja vakuuttamattomien riskien takia. Muita syitä kybervakuutuksen hitaaseen omaksumiseen vuonna 2013 oli se, että uskotaan että investoiminen kyberriskien ehkäisyyn on parempi kuin kybervakuutuksen ostaminen, markkinat ovat rajoitetut ja informaatio on puutteellista. (Zelle ym. 2014)

Kybervakuutusmarkkinoiden kasvusta sekä kybervakuutus tuotteen kysynnästä on ristiriitaisia mielipiteitä. Bandyopadhyay ym. (2009, 68) mukaan kybervakuutus ei ole ottanut odotettua suosiota IT-johtajien riskienhallinnan keinoissa. Kybervakuutusmarkkinoiden rajoittunut kasvu nähdään johtuvan usein kybervakuutustuotteiden konservatiivisesta hinnoittelusta, mikä johtuu markkinoiden kokemattomuudesta. Hyökkäyksien tappioista oleva vähäinen datan määrä, tuote- ja markkina kokemuksen puute sekä laskennalliset vaikeudet ovat johtaneet siihen, että vakuutusyhtiöt pelaavat varman päälle ja ylihinnoittelevat kybervakuutustuotteet. Epätäydellinen informaatio johtaa näin tuotteiden ylihinnoitteluun. Kilpailuilla markkinoilla ylihinnoitellut tuotteet asettuvat kysynnän tasolle ajan kuluessa. Kuitenkin kybervakuutus tuotteet ovat olleet yli vuosikymmenen markkinoilla ja ne ovat silti edelleen vajaakäytössä. Kysynnän puolen ongelmat ovatkin syvempiä kuin tarjonnan ongelmat ja näin ollen, ennen kuin kysynnän ongelmat ovat ratkenneet, eivät markkinat voi korjata itse itseään kybervakuutuksen kohdalla. Yang &

Luin (2014, 16) mukaan moraalikato on este kybervakuutuksen olemiselle kannustin tietoturva investointiin, silloin kuin kyberrikoksesta aiheutuva tappio on kokonaan vakuutettu.

Vain murto-osa toteutuneista kyberhyökkäyksistä tulee julkisuuteen. Riippuen maan lainsäädännöstä yritykset voivat käyttää omaa harkintaa siinä, informoivatko sidosryhmiä tapahtuneesta kyberhyökkäyksestä. Jos yrityksellä on kybervakuutus se voi hakea korvauksia, jolloin tieto kyberrikoksesta leviää yrityksen ulkopuolelle ja vahingoittaa yrityksen mainetta tai aiheuttaa muita seurauksia. Vaikka yritys ei julkaisisikaan tietoja kyberhyökkäyksestä, voi tieto levitä sidosryhmille puskaradion sekä riippumattomien analyysien kautta. Bandyopadhyay ym. (2009,73) tutkimuksen mukaan vakuuttajien olisi hyödyllistä laskea vakuutusmaksuja ja näin kasvattaa kybervakuutusmarkkinoita. Kybervakuutusmarkkinat ovat melko homogeeniset, koska yritykset joiden liiketoiminta perustuu isoilta osin tietojärjestelmiin, muodostavat suurenosan kybervakuutuksen kysynnästä. Tällöin vakuutusyhtiöt ovat paremmassa asemassa, kun markkinoilla on epäsymmetristä informaatiota.

4.3 Kybervakuutus ja kybervakuutusmarkkinat tänä päivänä

Kybervakuutus on muuttunut vuosien varrella samalla tavoin kuin kyberriskitkin ovat jatkuvassa muutoksessa. Vakuutusehtoja tehdessä vakuutusyhtiöt kiinnittävän enemmän huomiota kuinka paljon arkaluonteista tietoa yrityksellä on ja mihin se on tallennettu sekä miten. Toinen iso muutos on se, että vakuutusyhtiöt palkkaavat teknologiaspesialistin tai tekevät yhteistyötä kolmansien osapuolien kanssa. Tärkeää on kysyä avainkysymykset liittyen yrityksen turvallisuusjärjestelmiin, jotta voidaan löytää haavoittuvat kohdat. (Voelker 2015, 42–44)

Kuten on mainittu, kybervakuutus oli alun perin suunniteltu vastuuvakuutukseksi. Kuitenkin ensimmäisen osapuolen suojasta tuli tämän tuotteen keskipiste. NetDiligence tutkimuksen mukaan vakuutuskorvauksista 78 prosenttia menee kriisipalveluihin, jotka pitivät sisällään rikostutkimuksen ja luotto sekä henkilötietojen seurannan. Lopusta 22 prosentista 8 prosenttia käytettiin oikeusturvatoimiin, 9 prosenttia oikeudellisiin sovitteluihin, 2 prosenttia regulatiivisiin puolustuksiin ja maksuihin sekä prosentti PCI maksuihin. Kybervakuutuksen vakuutussuoja on paljon laajempi vuonna 2015 kuin esimerkiksi viisi vuotta sitten. Syynä kybervakuutuksen suojan lisääntymiseen on esimerkiksi vakuutusmeklareiden lisääntynyt tietoisuus tietomurroista ja niiden luonteesta. Kybervakuutus ja sen vakuutusehdot tulevat jatkamaan muuttumistaan. Vakuutuksenantajan velvollisuutena on pysyä mukana kyberriskien sekä kysynnän muutoksissa ja

tarjota vakuutussuojaa, joka vastaa näihin tarpeisiin ja ottaa huomioon myös teknologian jatkuva integrointi arkeen. (Voelker 2015, 44)

Kybervakuutuksen kattavuus riippuu vakuutusehdoista. Vakuutus voi sisältää kyberhyökkäyksen jälkeisten kulujen korvauksen sekä luottoseurantapalvelut. Nykypäivänä on myös hyvin erilaisia kybervakuutuksia erilaisille kyberriskeille mutta kybervakuutus markkinat ovat silti vielä kasvavat. Maantieteellinen sijainti vaikuttaa siihen, millaisia kybervakuutuksen muotoja on saatavilla. Eniten vaihtoehtoja on saatavilla Yhdysvalloissa, jossa vaihtoehtoja on huomattavasti enemmän kuin esimerkiksi Kanadassa, johtuen erilaisesta vakuutusmaksupohjasta. (Shackelford 2012, 354)

Kybervakuutusmarkkinat jatkavat kehittymistään jatkuvasti. Vakuutussuoja kehittyy uusien teknologioiden kehityksen myötä ja on kehitetty muun muassa ”Cloud failure extension”, joka vastaa pilvipalveluihin siirtymisestä ja siellä toimimisesta johtuvien häiriöiden takia liiketoiminnan keskeytymisestä aiheutuneista kuluista. (Jones 2015, 28)

Tänä päivänä vakuutusyhtiöt tarjoavat kybervakuutuksien ostajille kyberriskien ehkäisyyn työkaluja sekä konsulttipalveluita luodakseen lisäarvoa sekä samalla erottautuakseen kilpailijoista. Tappion ehkäisemispalvelut voivat sisältää muun muassa yrityksen infrastruktuurin haavoittuvuuden tarkastamisen, kyberturvallisuuden riskiarvioin, ”dark net:in” monitoroinnin, kolmansien osapuolien turvallisuuden luokittelun, vaarallisten IP-osoitteiden ja mobiilisovellusten eristämisen sekä työntekijöiden koulutuksen. Nämä työkalut auttavat ehkäisemään kyberhyökkäyksiä. (Jones 2015, 28)

Se, mikä vakuutussuojan taso on oikea, riippuu yrityksestä sekä toimialasta. Melkein kaikki kybervakuutuksen ostajat ostavat vastuu sekä ensimmäisen osapuolen suojan datan arvolle määritettynä. Myös neljä viidesosaa ostavat ensimmäisen osapuolen suojan kyberrikoksien tutkimisen sekä myös kiristyksen varalta. Noin puolet ostajista ostavat myös keskeytysvakuutuksen. Kun yritykset arvioivat nykyistä sekä tulevaa riippuvuuttaan tietojärjestelmistä niiden pitäisi myös uudelleen arvioida kybervakuutukseen kulutettavien rahamäärien lisäksi, millainen kybervakuutus on sopiva yritykselle. Siihen, kuinka kattavan kybervakuutuksen yrityksen pitäisi ostaa, ei ole yksiselitteistä vastausta. Siihen vaikuttavat yrityksen oma riskinottohalu, datan määrä, yrityksen koko ja mahdollisen maineenmenetyksen taso. Kybervakuutus markkinoiden jatkuvan kehityksen takia yritysten tulisi arvioida kybervakuutuksensa riittävyyttä vuosittain ja uudet vakuutustarjoukset pitäisi ottaa huomioon. (Jones 2015, 30)

Nykypäivänä kybervakuutusmarkkinat ovat yli 2 biljoonan dollarin arvoiset maailmanlaajuisesti. Yhdysvaltalaiset yritykset kattavat markkinoista noin 90 prosenttia. Kybervakuutusmarkkinoiden odotetaan kasvavan nopealla vuosivauhdilla ja seuraavan kymmenen vuoden sisään ne voivat saavuttaa yli 20 biljoonan dollarin arvon. Yhdysvalloissa kasvu on koko ajan käynnissä johtuen muun muassa uudesta datansuojelu lainsäädännöstä. Lainsäädännölliset muutokset tulevat vauhdittamaan kasvua myös muualla maailmassa. (Allianz) Esimerkiksi Euroopan tietosuojalainsäädännön uudistus tulee lisäämään yritysten vastuuta tietosuoja-asioissa. Tietosuoja-asetusta ja direktiiviä aletaan soveltaa vuonna 2018. (www.tietosuoja.fi)

Biener, Elign ja Wirfsin (2015, 147) mukaan lainsäädännölliset rajoitukset voivat ehkäistä tietyntyyppisiä vakuutusehtoja ja muun muassa monissa maissa sakkoja vastaan vakuuttaminen on kiellettyä. Lainsäädännön muutokset ovatkin vakuutusyhtiöille riski ja kyberriskien hankaluus sekä dynaaminen luonne voivat sisältää uhkan vakuutusyhtiöille. Asiantunteva vakuutusmeklari tietää, että tarkka ennustaminen vakuutussuojan tarpeellisuudesta ei ole mahdollista, mikä voi rajoittaa halukuutta myydä tuotetta. Tämä taas johtaa siihen, että vain tietyt vakuutusyhtiöt ovat halukkaita tarjoamaan tuotetta. Näillä kaikilla on negatiivinen vaikutus kybervakuutusmarkkinoiden kasvuun. Lisäksi esimerkiksi terveydenhoitoalalla ei välttämättä olla valmiita antamaan esimerkiksi potilastietoja kolmansille osapuolille, mikä taas tekee ongelmalliseksi vakuutusehtojen määrittämisen, koska tarvittavaa tietoa ei saada.

Kuitenkin IRMI (International Risk Management Institute) Betterley:n raportin mukaan kybervakuutusmarkkinat jatkavat kasvuaan eritoten terveydenhoitoalan sekä pk-yrityksien segmenteissä. Varsinkin terveydenhoitoalan järjestelmien myyjät ovat enenevissä määrin kybervakuutuksen ostajia. Vakuutusyhtiöt tarjoavat erikoistuneita kybervakuutustuotteita näille segmenteille. Toimiala on jaettu koon eli brutto vakuutusmaksutulon mukaan ja on seuraavanlainen: 1) rajoitettu määrä todella suuria vakuutusyhtiöitä, joiden vakuutusmaksutulot ylittävät 100 miljoonaa dollaria. 2) Useita vakuuttajia 50–100 miljoonan dollarin vakuutusmaksutuloilla. 3) Vielä useampia 25–50 miljoonan dollarin vakuutusmaksutuloilla. 4) Lukuisia vakuuttajia 10–25 miljoonan dollarin vakuutusmaksutuloilla ja 5) Useita 5-10 miljoonan sekä 1-5 miljoonan dollarin vakuutusmaksutuloilla. (Betterley, 2015)

Vakuutuksenottajat jakautuvat selkeästi isoihin paljon kyberhyökkäyksiä kohtaaviin yrityksiin kuten terveydenhuoltoala sekä jälleenmyyjät, ja niihin yrityksiin, joiden kyberhyökkäyksien esiintymistiheys ei ole niin suuri. Yhdysvalloissa finanssisektori käsittää oman erillisen ryhmän, jonka vakuutukset hoidetaan erikseen. Tutkimukseen osallistuneista vakuutusyhtiöistä

melkein puolet raportoivat 26–50 prosentin kasvun kybervakuutustuotteiden vakuutusmaksuissa. Vain yksi vakuutusyhtiö raportoi negatiivisesta kasvusta, tämä johtui kuitenkin siitä, että yhtiö ei ole keskittynyt suuriin yhtiöihin sekä uudelleensuunnitteli kybervakuutuksen vakuutusehtoja. 2015 vuoteen asti kybervakuutusmarkkinoilla uudet vakuuttajat taistelivat markkinaosuuksistaan ja näin muodostui hintakilpailua. Kasvu johtui suurimmaksi osaksi, ellei kokonaan, uusista vakuutetuista yhtiöistä. 2015 vuoden jälkeen kasvun tekijät ovat muuttuneet ja kasvu on johtunut terveydenhoitoalan sekä jälleenmyyjien merkittävästi kasvaneesta kiinnostuksesta kybervakuutusta kohtaan. (Betterley, 2015)

Osa hintojen noususta on myös korvautunut suurimmilla vakuutuksenottajien omavastuuosuuksilla. Vakuutusmaksut ovat myös kasvaneet, koska vakuutetut valikoivat korkeammat korvausrajat ja ostavat lisäsuojaa esimerkiksi kiristyksen varalle. Taas Betterleyn (2015) mielestä kybervakuutusmarkkinat ovat kasvaneet, mutta hintakilpailu on suurimmaksi osaksi hävinnyt. Kyberrikosten kasvu aiheuttaa tulevaisuudessa yhä enemmän korvausvaatimuksia. Tämä korvausvaatimusten lisääntyminen voi olla vakuutusyhtiöille mahdollisuus vastata tietomurtoihin kustannustehokkaammin, kun vakuutusyhtiöt neuvottelevat matalammat vastuukustannukset ja lakiyhtiöt saavat enemmän kilpailua hinnoitteluunsa.

Kybervakuutuksen ostajat jaettiin siis kahteen osaan 1) isot yhtiöt, terveydenhuolto sekä jälleenmyynti ja 2) kaikki muut paitsi finanssisektori. Ensimmäiseen osaan kuuluville kybervakuutuksien hinnat ovat nousussa. Betterleyn (2015) tutkimuksen mukaan hintojen nousu vaihtelee 5-50 prosentin luokan välillä, yleisimmin kuitenkin 10–25 prosentin alueella. Jos yrityksillä on jo ennestään korvausvaatimus taustaa kyberriskeistä voi hintojen nousu olla jopa 200 prosenttia. Pk-yrityksille markkinat ovat paljon suopeammat ja hinnat ovat kilpailulliset. Pk-yritysten vaateet ovat olleet maltillisia, mutta tämä tulee varmasti tulevaisuudessa muuttumaan, kun yritykset kärsivät tietomurroista, jotka johtavat suurempien yrityksien vastuukorvauksiin sekä maksukorttiteollisuuteen. Vakuutusyhtiöt vastaavat lisääntyneisiin kyberhyökkäyksiin käyttämällä yhä tarkempia vakuuttamistyökaluja, tarjoamalla riskienhallintapalveluita vakuutuksenottajille sekä siirtämällä enemmän riskiä jälleenvakuuttajille. Jälleenvakuuttajat ovat enenevissä määrin kiinnostuneita kybervakuutustuotteista.

Betterleyn (2015) mukaan kyberturvallisuus on selkeä tämän päivän trendi markkinoilla. Ympäri maailmaa pidetään paljon kyberriski seminaareja ja konferensseja, jotka ovat täynnä vakuutusyhtiöiden edustajia, meklareita, asianajajia sekä mahdollisia tulevia kybervakuutuksen ostajia, jotka ovat kiinnostuneita kyberturvallisuudesta. Kiinnostuksesta seuraa yleensä tuotteen

ostaminen, mikä vaikuttaa vakuutusmarkkinoihin korkeampina vakuutusmaksuina tai omavastuuosuuksina.

5 KYBERRISKIT JA KYBERVAKUUTUSMARKKINAT SUOMESSA

5.1 Haastateltavien esittely

Tämä luku kattaa tutkimuksen empiirisen osion, eli asiantuntijahaastattelut ja luku on kirjoitettu teemahaastattelujen pohjalta. Haastatteluja tehtiin yhteensä kuusi kappaletta, joista yksi suoritettiin heinäkuussa 2016, kolme joulukuussa 2016 ja kaksi tammikuussa 2017. Haastateltavien valinnassa keskityttiin löytämään haastateltavia, joiden tietojen avulla saataisiin mahdollisimman kattava käsitys suomalaisten yritysten kyberriskeihin varautumisen keinoista sekä Suomen kybervakuutusmarkkinoiden tilasta ja itse kybervakuutuksesta vuonna 2016.

Haastattelin kahta suomalaista yritystä, kolmea vakuutusyhtiötä ja yhtä vakuutusmeklari yritystä. Kaikki haastattelut nauhoitettiin haastateltavien suostumuksella ja haastattelujen kesto vaihteli yhdestä kahteen tuntiin. Haastateltavien nimiä ei ole mainittu tässä tutkimuksessa, koska osa haastateltavista ei tiedon arkaluontoisuuden sekä heidän tunnistettavuuden johdosta halunnut olla nimellä tutkimuksessa. Jotta tutkimus olisi mahdollisimman selkä ja yhdenmukainen, kaikki haastateltavat esiintyvät anonyymisti tutkimuksessa. Yrityksien nimiä ei ole myöskään mainittu tunnistettavuuden takia. Vakuutusyhtiöiden osalta nimet ovat mainittu, koska he eivät tuoneet julki mitään kriittistä tietoa, jonka julkaisemisella voisi olla vaikutusta liiketoimintaan ja suurinosa haastatteluista tulleesta tiedosta on julkista. Vakuutusyhtiöistä yrityksien nimillä puhuminen myös helpottaa lukijaa tutkimuksen seuraamisessa. Kyberturvallisuuden varmistamisesta ja kyberriskeihin suojautumisen keinoista on kerrottu tässä tutkimuksessa vain yleisellä tasolla, jotta mitään yrityksille kriittistä tietoa ei paljastettaisi. Haastateltavat on nimetty A-F kirjainten avulla, jotta tutkimuksen seuraaminen ja lukeminen olisi sujuvampaa.

Haastateltava A toimii ITC-johtajana suomalaisessa yhtiössä. Hänellä on kymmenien vuosien kokemus tietojärjestelmistä ja hän on myös työskennellyt vakuutusyhtiöissä sekä IT-konsul-

tointi yrityksessä. Koulutukseltaan hän on yhteiskuntatieteiden maisteri tietojärjestelmätieteistä. Lisäksi hänellä on EMBA tutkinto Jyväskylän Yliopistosta. Hän on myös ollut mukana monissa kyberturvallisuuteen liittyvissä ryhmissä ja tehnyt paljon yhteistyötä muun muassa yliopiston sekä ammattikorkeakoulun kanssa kyberturvallisuuteen suuntautuvassa pääaineessa. Haastateltava A:lla on näin ollen erittäin laaja näkemys kyberturvallisuudesta ja siitä, miten se on organisoitu yhtiössä, jolla on hyvin paljon arkaluonteista tietoa.

Haastateltava B on keskisuuren pörssiyrityksen tietojärjestelmäarkkitehti. Hänen koulutustaustansa on tietotekniikkamekaanikko ja hän on työskennellyt useita vuosia automaatiotekniikan parissa. IT-osastoilla hän on työskennellyt muun muassa Valmetilla sekä Metsolla ja tehnyt laaja-alaisesti erilaisia tietojärjestelmiin liittyviä töitä. Haastateltava B tuo empiriaan näkökulmaa pk-yrityksen tietojärjestelmäarkkitehtuurista sekä siitä, miten siellä on huomioitu kyberriskit yritystä uhkaavana tekijänä.

Haastateltava C toimii vakuutusmeklarina Aon vakuukuutusmeklarointi yrityksessä ja koulutukseltaan hän on ekonomi. Aonilla hän johtaa tällä hetkellä vakuutusmeklari tiimiä. Hän on luonut kansainvälistä uraa vakuutusliiketoiminnan parissa ja työskennellyt Marshilla niin Englannissa kuin Suomessakin. Aon on maailman suurin riskienhallinta- ja vakuutusvälityspalveluja sekä henkilöstöetuuskonsultointia yrityksille tarjoava palveluntuottaja. Aonin liiketoiminta on maailmanlaajuisesti organisoitu verkostoksi, joka toimii 120 maassa ja jossa työskentelee 72 000 asiantuntijaa. Suomessa toimiva Aon konsernin tytäryhtiö Aon Finland Oy on keskittynyt suuriin yrityksiin, joten hänen vastauksissaan tulee vahvasti esiin suuryritysten näkökulma.

Haastateltava D työskentelee If vakuutusyhtiössä ja hän on koulutukseltaan juristi. Hän on työskennellyt erilaisissa tehtävissä vakuutusyhtiössä noin 15 vuotta. Hän on ollut tuotepuolella pitkään niin yritys- kuin yksityisvakuutuksissa sekä tehnyt riskivalintaa. Hänellä on myös neljän vuoden kokemus vastuuvakuutuksista, minkä hän näkeekin juristin työlle erittäin luontevana, koska niissä tuotteissa vakuutetaan vahingonkorvausvelvollisuutta. If tekee yhteistyötä kybervakuutuksissa teknologiayhtiö IBM:n kanssa. Haastateltava D:n näkemys kybervakuutuksesta kattaa niin pienten kuin suurtenkin yrityksien näkökulman, koska IF myy tuotetta suuryrityksien lisäksi myös pk-yrityksille.

Haastateltava E työskentelee kansainvälisessä AIG vakuutusyhtiössä ja on koulutukseltaan myös juristi. Hän on ollut eri vakuutusyhtiöissä töissä noin 13 vuotta ja hän on työskennellyt underwriting puolella ja myös vastuuvakuutusten parissa. Hänen näkemyksensä on kyberris-

kien osalta enemmän juridinen kuin tekninen. AIG on yksi maailman johtavista vahinkovakuutuskonserneista, joka palvelee asiakkaita yli 130 maassa, ja jonka palveluksessa on noin 40 000 työntekijää ympäri maailmaa. Suomessa AIG:n palveluksessa on yli 50 asiantuntijaa, jotka vastaavat yksilöllisten vakuutusratkaisujen räätälöinnistä ja vahinkojen hoidosta. AIG tekee yhteistyötä kybervakuutuksien osalta teknologiayhtiö Nixu Oyj:n kanssa, joka on profiloitunut nimenomaan kyberriskeihin erikoistuneena IT-konsultointiyrityksenä. Haastateltava E:n vastauksissa painottuu kybervakuutuksen myynti nimenomaan suurille asiakkaille sekä juridinen näkökulma.

Haastateltava F toimii yksikön päällikkönä OP Pohjola vakuutusyhtiössä ja on koulutukseltaan juristi. Tämän lisäksi hänellä on myös EMBA tutkinto ja vakuutusyhtiössä hän on työskennellyt noin 15 vuotta. Hänen vastuualueinaan on myös ollut suurasiakas kybertuotteen kehittäminen ja hän on ollut mukana asiakkaille järjestettävissä kyberturvallisuus-seminaareissa. Hän on työskennellyt vakuutusyhtiössä underwriting-tuki sekä lakiasioissa ja viimeiset viisi vuotta jälleenvakuutus ja kansainvälisissä asioissa.

Teemahaastattelut toimivat tässä tutkimuksessa pääasiallisena empiirisen aineistonkeruumenetelmänä. Teemahaastatteluille tyypillisesti haastatteluissa käsiteltiin tiettyjä aiheita syvällisemminkin ja haastateltavat toivat keskusteluun huomioita myös kysymysten ulkopuolelta. Yrityksille esitetyt kysymykset koskivat kyberriskejä ja vakuutusyhtiöiden edustajille esitetyt kysymykset taas kybervakuutusta sekä kybervakuutusmarkkinoita Suomessa. Yrityksille tehtyjen haastattelun avulla kartoitettiin erilaisten suomalaisten yrityksien kyberriski ja -vakuutus tietoisuutta ja kyberriskeihin varautumiskeinoja. Vakuutusyhtiöiden edustajille suoritetuissa haastatteluissa taas pyrittiin saamaan kuvaa Suomen kybervakuutusmarkkinoista sekä kybervakuutuksesta tuotteena vakuutuksenantajan näkökulmasta.

Aineiston tulkinnassa pyritään keskittymään teorian luomiin puitteisiin, mutta annetaan tilaa uusille näkökulmille ja ilmiöille. Teoria ohjasi myös haastattelukysymysten luomista, joten se näin vaikutti myös aineiston muodostumiseen. Kaikille haastateltaville ei esitetty kaikkia kysymyksiä samassa järjestyksessä, jos haastateltava toi itse esille kysymyksissä ilmenneitä seikkoja jo aikaisemmin. Teemahaastattelulle ominaisesti keskustelu oli myös hyvin vapaata haastattelujen aikana ja tämän myötä saatiin myös keskusteluun nostettua asioita ja uusia näkökulmia, joita haastattelurungossa ei ollut.

Haastattelurunkoja (liite 1.) tehtiin yhteensä 4 kappaletta. Haastattelurunkoja (liite 2.) tehtiin yhteensä 2 kappaletta. Haastattelut suoritettiin yksitellen ja haastattelurungon teemat painottuivat haastateltavan asiantuntemuksen mukaan. Haastattelujen nauhoitukset litteroitiin tekstimuotoon sähköisesti, jonka jälkeen aineistosta pyrittiin löytämään yhtäläisyyksiä ja tiiviimpi kuvaus teemoittain. Haastattelut litteroitiin sanatarkasti, joten niistä on pystytty ottamaan sanatarkkoja lainauksia haastateltavilta, mikä lisää osaltaan tutkimuksen luotettavuutta. Seuraavassa luvussa analysoidaan tutkimuksen empiiristä aineistoa eli haastatteluista saatua tietoa ja luku on jaoteltu teemoihin haastattelurungon kysymyksiä mukaillen. Teemoittelun avulla on saatu aineistosta eri haastateltavien mielipiteitä koottua yhteen ja näin ollen aineistosta on saatu tutkimusongelmien kannalta olennaiset seikat esille. Teemoittelu myös jäsentää haastatteluista kerättyä tietoa ja näin ollen helpottaa empiirisen aineiston lukua.

5.2 Kyberriskit ja niihin varautuminen Suomessa

5.2.1 Kyberriskeiltä suojautuminen

Tietoturvaa on Suomessa aina pidetty tärkeänä jo vuosikymmeniä ja muutama vuosi sitten tuli kyber-sana mukaan. Voidaankin nähdä, että kyberturvallisuus on tavallaan tietoturvan kyljessä. Kyberriskit ja niiden havaitseminen ovat nousseet Suomessa trendin omaisesti viimeisen 2 vuoden aikana. Osa yrityksistä pitää kyber-sanaa trendi-sanana ja näkevät sen pitävän sisällään perinteistä tietoturvaa. Suuret yritykset, joilla on paljon arkaluonteista tietoa, ovat jo pitkään kehittäneet tietoturvaansa sekä kouluttaneet henkilöstöä toimimaan oikein ja huolellisesti. Haastattelemieni yritysten edustajat näkevätkin, että on tavallaan vaan keksitty uusi sana, jolla saadaan jo ollut asia nostettua tapetille ja pysymään siellä. Lisäksi tämän avulla saadaan tietoturvaa nostettua sille tasolle, missä sen nykypäivänä pitäisi ollakin. Vakuutusyhtiön edustajat taas ovat asiasta eri mieltä ja kyberin nähdään sisältävän paljon muutakin kuin vain perinteistä tietoturvaa. Kaikki laitteet ovat kytkettyinä internetiin ja yhä enemmän palveluita tulee olemaan pilvessä, joten riski on jatkuvasti kasvava ja paljon suurempi kuin perinteinen tietoturvakäsitys. Riski on myös muuttuva, koska tietotekniikka kehittyy jatkuvasti mikä taas mahdollistaa yhä erilaisempia kyberrikoksia.

Haastateltava E painottaa, että ihmiset tekevät rahaa kyberrikollisuudella, joku palkkaa henkilön, joka tekee hyökkäyksiä. Massiivisuus on tässä ongelma eli kuinka paljon yks asia voi vaikuttaa niin moneen asiaan. Rikollisten kyvykkyydet kehittyvät, mitä enemmän tietojärjestelmätkin kehittyvät ja kyse ei näin ollen ole enää perinteisestä tietoturvasta. Haastateltava F huomauttaa, että tietoturva on vaan vastuuosio, mutta on olemassa myös keskeytysosio. Tietoturva on siinä vaiheessa ihan sama, jos asiakastiedot häviävät. Hänen mielestään on kummallista, että kukaan ei näytä miettivän sitä maineen menetystä, jos asiakastiedot vuotavat nettiin. Jos asiakas ei enää luota, se on massiivinen riski.

Haastateltava A näkee kyberin myös hyvin paljon yhteiskunnallisena asiana. Kyberille on ollut, on ja tulee olemaan monta merkitystä. Mikä erottaa sen normaalista tietoturvasta on muun muassa se, että vastapuolella on äärettömän paljon rahaa käytössä eli on käytännössä valtiollinen toimija, joka hyökkää. Suomessa kyberturvallisuus liittyy yhteiskunnan turvallisuusstrategiaan eli sähköverkot pysyvät päällä ja pankit toimivat. Haastateltava A kokee kyberturvallisuudesta huolehtimisen ja tiedottamisen myös paljon yhteiskunnan vastuulla olevana, ja tätä kautta myös yritysten tietoisuus ja valmiustaso lisääntyvät.

Kyberriskien asema Suomessa on sillä tasolla, että yritykset tulevat jatkuvasti yhä tietoisimmiksi riskeistä sekä mitä vaihtoehtoja niiltä suojautumisessa on. Hyvin monet yritykset ovat tietoisia siitä, että esimerkiksi väärennettyjä sähköposteja lähetellään toimitusjohtajan nimissä, mutta liiketoiminnan keskeytysriskille altistumisesta ei olla vielä niin tietoisia tai ei osata arvioida tätä riskiä ja sen suuruutta. Haastateltava C erittelee kyberriskit kolmeen osa-alueeseen: ensimmäisessä on liiketoiminnan keskeytysriski, toisessa taas kiristysriski ja kolmannessa osa-alueessa on vastuuriski eli jos menettää kolmannen osapuolen tietoja ja joutuu korvausvastuuseen. Vastuuriskille altistuminen on kuitenkin haastateltavan mielestä Suomessa vähäistä verrattuna muihin maihin kuten esimerkiksi Yhdysvaltoihin.

On eriäviä mielipiteitä siitä, kuinka hyvin lisääntyvät kyberriskit ovat tiedostettu yritysten keskuudessa. Haastateltava A:

”Isoissa kohtuullisesti ja pienissä ei ollenkaan ja kuntasektorilla ei ollenkaan tai vaikka ois tunnistettu niin ei ole toimittu ollenkaan. Yliopistot aina ollut karmeita paikkoja, ei oo heikentynyt, kun ei koskaan ole ollutkaan millään tasolla. Ilmoitustauluilla on salasanat ja käyttäjätunnukset koneille. Täysin turvattomia ovat yliopiston työasemat.”

Kaikki haastateltavat olivat yhtä mieltä siitä, että isoimmissa yrityksissä on tunnistettu kyberriskit paremmin kuin pienissä ja keskisuurissa. Haastateltava B täsmentää vielä, että tietoisuus

kyberriskeistä menee yleensä yrityskoon mukaan. Ihan pienimmät yritykset käyttävät pilvipalveluita ja heillä ei näin ole omia palvelimia ollenkaan. Seuraavassa kokoluokassa alkaa olla omia palvelimia, mutta yleensä vain muutama ihminen huolehtimassa niistä ja muista asioista samaan aikaan sekä yleensä tässä kokoluokassa ei myöskään ole kumppaneita. Kun verrataan seuraavaan kokoluokkaan, jossa yrityksessä on oma IT-osasto ja voi olla jo partnereitakin, on kyberriskeistä huolehdittu jo aivan eri tasolla.

Kyberriskeihin varautumisessa käytetään erilaisia riskienhallinnan muotoja riippuen yrityksestä. Haastateltava A alleviivaa, että henkilöstön koulutus on erittäin tärkeässä roolissa ja onkin vaikea sanoa, kuinka monta prosenttia hyökkäyksistä johtuu siitä, että henkilökunta on mennyt ikäville sivuille joista tuo viruksia. Organisaatiossa A tämä on estetty sillä, että peruskäyttäjän oikeudet eli käyttövaltuudet on rajatut ja ne ovat vain sellaiset mitä tarvitsee työssä. Henkilökunnan ei siis tarvitse työtä varten asentaa työasemille mitään.

Työasemilla ei ole esimerkiksi pelejä tai mitään muuta kuin työntekoon edellyttävät ohjelmat. Tietoturvakurssit ovat isoimmissa organisaatioissa olennaisessa osassa henkilöstön tietoturvaosaamisen kouluttamisessa. Organisaatiossa A on jo vuosikymmeniä kehitetty tietoturvaa niin osaamista, koulutusta kuin apuvälineitäkin. Yrityksellä on paljon arkaluonteista tietoa, ja jos niihin joku pääsisi käsiksi, olisi maineriski valtava. Maineriskiä ja asiakkaiden luottamusta pidetäänkin yhtenä tietoturvauhkan osa-alueista, ja sitä pyritään käsittelemään hyvin kattavasti.

Organisaatio B jakaa kohtaamansa kyberriski ulkoisten digipalveluiden tuomiin riskeihin, jotka ovat Amazon palvelussa, ja konsernin sisäisiin riskeihin. Sisäisiä riskejä ovat esimerkiksi työasemat ja näihin riskeihin luetaan muun muassa sähköpostin kautta tulevat huijaukset sekä, jos internetissä mennään väärille sivuille tai asiakkaan USB-tikun mukana tulee haitakesovelluksia.

Molemmat organisaatiot panostavat paljon tietoturvaan ja suurimmaksi osaksi samoin keinoin. Normaali tietoturvatausta on palomuurit, virustorjunta ja liikenteen filtterointi. Kaikki liikenne skannataan ja profiloidaan ja sisään ei päästetä sellaisia tiedostoja, jotka voisivat mennä suoritukseen esimerkiksi exefilet. Organisaatio A:lla on myös kumppani, jonka kanssa tekee yhteistyötä tietoturva asioissa ja jolta saa ilmoituksia havaituista riskeistä. Esimerkiksi tietoturvahavainnon sattuessa toimenpiteet alkavat heti ja työasemia eristetään verkosta. Heillä on myös varmistus ja palautus rutiinit siltä varalta, jos joku laittaa työasemat lukkoon. Hävinneitä tietoja pystytään myös palauttamaan palvelimilta.

Eroja kyberriskeihin suojautumisesta löytyi työntekijöiden käyttövaltuuksista. Organisaatio A:lla käyttövaltuudet olivat hyvin rajattuja ja työasemille ei pysty työntekijät lataamaan mitään sovelluksia, eikä käyttämään konetta mihinkään muuhun kuin työntekoon. Organisaatio B:llä taas työntekijät voivat ladata työasemille ohjelmia. Kaikki työntekijät pystyvät organisaatiossa lataamaan kaikkea ja yrityksessä on käyttöoikeuksien osalta vaihteleva käytäntö vanhastaan, osalla enemmän osalla vähemmän oikeuksia. Haastateltava B:n mielestä osalla käyttäjistä on turhankin paljon oikeuksia. Taidosta ei hänen mukaansa kuitenkaan ole nykypäivänä kyse, jos vaan sattuu vahingossa menemään ja klikkaamaan väärästä paikasta.

Henkilöstön näkeminen riskitekijänä koettiin myös erilaiseksi. Organisaatio A näkee henkilöstön suurena riskitekijänä ja kokee näin henkilöstön tietoturvakoulutuksen erittäin tärkeäksi ja on panostanut siihen, kun taas organisaatio B ei ole järjestänyt vielä henkilöstölleen esimerkiksi tietoturvakoulutuksia. Haastateltava B:n mukaan henkilöstö riskitekijänä ei ole iso ongelma ja koulutuksellakaan ei välttämättä aina saada toivottuja tuloksia.

Esimerkiksi hän ottaa yhtiön tulostuksessa tapahtuneen kyberhyökkäyksen. Tulostuksessa odotettiin tiedostoa, jossa piti olla liitetiedosto mukana. Tiedosto saapui, mutta se ei suinkaan ollut se tiedosto mikä piti. Työntekijät avasivat sen sitten ajattelematta, koska tiesivät odottaa tiedostoa. Tiedosto sattui sitten olemaan ransomware, josta koko kone meni tukkoon. Tämä aiheutti myös vahinkoa muille palvelimella oleville levyille, joten vahinko ei jäänyt koskemaan vain yhtä konetta. Välttämättä ei siis koulutuskaan auta vaan kokemus, kun on kerran sattunut nii tietää sitten jatkossa samankaltaisissa tilanteissa. Tässäkin tapauksessa tiedosto oli livahtanut sähköposteista läpi niin, että filtterit eivät olleet saaneet sitä kiinni. Hänen mukaansa riskit välttää parhaiten, jos on ylivarovainen koko ajan, mutta sekään ei työelämässä kuitenkaan aina onnistu.

Organisaatio A:lla on vuosittaiset tietoturvakoulutukset, jotka ovat tärkeässä roolissa tietoturvariskien tietoisuuden levittämisestä henkilöstölle ja tätä kautta parannetaan henkilöstön valmiutta työskennellä vastuullisesti. Koko henkilöstöllä on pitkä kurssitus tietoturvasta, joka on pakko tehdä tietyn ajan kuluessa työskentelyn aloitettua. Organisaatio B:llä ei ole tietoturvakoulutuksia henkilökunnalle, mutta haastateltava koki ne ehdottoman tarpeelliseksi, koska käyttäjillä ei ole kunnon ohjeistusta tai koulutusta tällä hetkellä liittyen tietoturva-asioihin. Organisaatio on uusimassa IT-strategiaansa, jonka myötä vuodelle 2017 on tulossa loppukäyttäjille uusi ohjeistus ja tietoturvakoulutus.

Yleisinä tietoturvariskienhallintakeinoina pidetään salasanojen pakottamista tiettyyn formaattiin ja niiden uusimista säännöllisin väliajoin. Organisaatiossa A tehdään myös tietoturva auditointeja, jossa ulkopuolinen auditoija tekee hyökkäysyrityksen ja yrittää kaikilla keinoilla päästä sisään tietoturvan läpi. Jos huomataan jotain puutteita, niin niitä korjataan auditoinnin jälkeen ja näin vahvistetaan tietosuojaa. Työasemien lukittautumisen varalta työasemille ei viedä mitään tietoja ja näin ollen kaikki tiedot ovat varmistetuilla palvelimilla, joista ne pystytään palauttamaan.

Molemmat organisaatiot käyttävät jossain määrin black tai white listauksia kyberriskien hallintakeinoina. Organisaatiossa B:ssä taas blogataan pois malware sitet, mitkä tunnistettu ja mistä tulee haitakesovelluksia. Organisaatiossa A ei ole pitkään aikaan blogannut sivustoja eli black listauksesta on luovuttu ja white listausta he eivät ole koskaan käyttäneetkään yleisesti, vain tietyissä erikoistyöasemissa.

Molemmat organisaatiot ovat kärsineet kyberhyökkäyksistä. Haastateltava B kertoo viimeisimmästä huijausyrityksestä, jossa talousjohtajalle tuli sähköpostiviesti mukamas toimitusjohtajan sähköpostista. Viestissä pyydettiin tekemään 21 000 euron siirto jonnekin, mutta koska viesti oli epämääräisesti kirjoitettu, se kärähti siinä. Toimitusjohtajien nimissä lähetetyt huijaussähköpostit ovatkin melko yleisiä nykypäivänä. Haastateltavien mukaan kyberhyökkäyksissä on kuitenkin nähtävissä tietynlaisia trendejä ja näin ollen riski on jatkuvasti muuttuva. Esimerkiksi kaksi vuotta sitten ei ollut vielä niin paljoa ransomwareja eli kiristysohjelmia, kuin tänä päivänä. Haastateltava B näkee ransomwaret nykypäivän trendinä ja suurimpana uhkana, koska niitä saadaan läpi paljon enemmän kuin aikaisemmin. Ennen oli paljon palvelunestohyökkäyksiä (denial of service), mutta nykyään niitä on taas vähemmän. Palvelunestohyökkäyksellä ei tietynlaisiin organisaatioihin pystytä aiheuttamaan välttämättä minkäänlaista haittaa toisinkuin ransomwareilla. Kyberriskien kehityksessä onkin näkyvissä se, että ne ovat yhä haitallisempia ja aiheuttavat enemmän kustannuksia organisaatioille.

Haastateltava A:n kokemuksen mukaan hyökkäysyritysten määrä on todella suuri ja koputtelujen määrä vielä suurempi. Muun muassa selaimen avulla yritetään tehdä get pass worldfile:ja. Haastateltava A painottaa, että jatkuvasti joutuu seuraamaan enemmän, jolloin rahaa menee sen seurauksena myös enemmän. Hänen mukaansa on pakko olla 24 tuntia vuorokaudesta valvonnassa, jotta riskiä pystytään kontrolloimaan riittävällä mittakaavalla. Hyökkäykset käynnistyvät pääasiassa juhlapyhinä, jolloin frekvenssi hyökkäyksissä voi jopa kymmenkertaistua. Juhlapy-

hinä käynnistyviin hyökkäyksiin liittyy se, että hyökkääjät ajattelevat yritysten olevan huonoiten miehitetty ja näin ollen heikoimmin valvottu ja helpompi kohde hyökkäyksille. Lisäksi myös esimerkiksi koulujen koneita on enemmän vapaana ja hyökkäyksiä pystyy käynnistämään tämän johdosta tehokkaammin.

Organisaatiossa A on erillinen tietoturvatiimi, jossa on noin 20 henkilöä. Tietoturvatiimi hoitaa tietoliikennettä, tietoturvaa sekä käyttövaltuusasioita. Lisäksi heillä on tietoturvan osaamisryhmä, joka auditoi sovelluksia, kun niitä rakennetaan ja tarkistaa, että kaikki olennaiset asiat otetaan huomioon. He näkivät myös erittäin tärkeänä, että koko organisaatiolla on käsitys tietoturvasta ja sen tasosta ja riskeistä. Heidän organisaatiossaan on kyberturvallisuusjohtaja, jonka päätehtävä on huolehtia, että kaikki suunnitelmat ovat kunnossa esimerkiksi auditoinnin osalta. Heillä on myös tietoturvapäällikkö, joka operoi kaikkea tietoturvaa, valmiusasioita ja lisäksi vastaa yleisestä riskienhallinnasta. Hänen tehtävänsä on myös huolehtia, että kyberturvariskit ovat siedettävällä tasolla. Riskienhallinnassa he hakevat nimenomaan rahan ja riskin tasapainoa, kuinka iso riski on ja kuinka paljon rahaa siihen laitetaan. Organisaatio järjestää myös kyberturvallisuusseminaareja, joihin koko johtoryhmä osallistuu. Organisaatiossa A on siis hyvin kattava kyberturvallisuusosaaminen ja siihen on panostettu paljon.

Organisaatio B koki myös tärkeäksi, että tieto kyberriskeistä ja niiden hallinnasta on myös ylimmällä johdolla ja hallituksella. Tässä organisaatiossa on myös erillinen IT-osasto, joka huolehtii yrityksen tietojärjestelmistä ja niiden toimivuudesta. Kyberhyökkäyksen sattuessa he paikantavat hyökkäyksen ja korjaavat tiedostot. Talousjohtaja vastaa viimekädessä riskienhallinnasta ja talousjohtajan alla vastuussa olevana toimii tietohallintopäällikkö.

Haastateltava A näkee kyberriskit samassa asemassa kuin muutkin riskit. Hän vertaa kyberriskiä esimerkiksi tulipaloriskiin, samalla tavalla kyberriski on olemassa, vaikka todennäköisyys tapahtumalle on pieni, mutta riski on todella iso ja sitä pyritään pienentämään kaikilla mahdollisilla keinoilla. Tietokoneiden tuhoutumiseen liittyvää paloriskiä, pienennetään muun muassa sillä, että konesalitiloihin ei saa viedä mitään mikä voisi syttyä, esimerkiksi paperia. Tiettyihin tiloihin on myös rajoitetut kulkuoikeudet. Hän kuitenkin näkee, että kyberturvallisuus ei voi koskaan olla täysin kunnossa ja siinä mielessä ehkä tärkeämmässä asemassa kuitenkin kuin muut riskit, koska sitä joudutaan aktiivisesti kehittämään koko ajan.

Haastateltava B:n huomauttaa, että fyysisiin riskeihin on totuttu varautumaan ja niin ne ovat paremmalla tolalla kuin tietoturvariskeihin varautuminen, vaikka siihenkin panostetaan paljon.

Muihin riskeihin varatutumisesta on tullut vuosien myötä automatiikkaa. Tietoturvariskeihinkin varautumisesta on osittain jo tullut automatiikkaa, mutta helposti ollaan välinpitämättömiä ja ajatellaan että tämä on vain digivirtaa.

Kun puhutaan kyberriskien tulevaisuudesta, tuli monesti esille se, että tapahtumat tulevat olemaan suurempia ja niitä tulee olemaan jatkuvasti enemmän. Melkeinpä mahdottomaksi osoittautui sanoa, millaisia uusia riskejä tulevaisuudessa tulee olemaan, koska riskin luonne on jatkuvasti muuttuva, kun teknologia kehittyy eikä riskejä juurikaan pysty ennustamaan. Haastateltava A kiteyttää, että riski tulee kasvamaan ilman muuta sen takia, että vastapuolen menetelmät kehittyvät ja Suomessakin on tietyissä piireissä nähty oikeata vakoiluakin. Kyvykkyydet ja potentiaalisten ihmisten määrä kasvavat ja on mahdollista ostaa hyökkäys jotain yritystä vastaan sekä rakennella suunnattuja hyökkäyksiä paremmin.

Molemmat organisaatiot näkivät kyberriskien merkityksen kasvavan tulevaisuudessa. Sitä mukaan, kun perinteinen liiketoimintamalli vähenee ja asiat ja asiakkaat siirtyvät enemmän verkon puolelle, lisääntyy näin ollen luonnollisesti myös riskit. Toimintatapoihin lisääntyneet riskit ovat jo aiheuttaneet muutoksia. Organisaatio B on hajauttanut riskiä siirtämällä osan palveluistaan pilvipalveluihin ja osa on säilytetty omilla palvelimilla. Näin ollen, jos toiseen hyökätään, pystytään toisella vielä ylläpitämään normaali liiketoiminta taustalla.

5.2.2 Kybervakuutuksen osto

Molemmat haastateltavat olivat sitä mieltä, että vakuutusyhtiöt ovat varmaan säästäneet markkinointikustannuksissa, koska tuotteen tunnettuus on ollut niin huonoa. Kummallakaan yrityksellä ei ollut kybervakuutusta eivätkä he olleet siitä kuulleet aikaisemmin. Haastateltava A lisäsi, että he tuskin tulisivat sitä aivan lähitulevaisuudessa ottamaankaan. Tietoisuus tuotteesta oli hyvin huono ja haastateltavat eivät uskoneet siihen, että tuote tulisi Suomessa menestymään tulevaisuudessakaan kovin hyvin. Haastateltava A ei myöskään uskonut, että Suomessa syntyisi kauheasti kilpailua tuotteen tarjoajien kesken ja että tuotetta on turha tarjota pk-yrityksille, ainoastaan suuryrityksille, jos niillekään. Hän myös parantaisi tietoturvaa entisestään kybervakuutuksen oston sijaan. Vahingon arvoa on hyvin vaikea määrittää eikä hän senkään perusteella usko, että tuote tulee Suomessa menestymään.

Suomessa on vähän maksajia, joten vakuuttaminen on kallista. Yhdysvalloissa esimerkiksi taas on paljon maksajia, joten tuote menestyy siellä aivan eri tavalla. Koska kysymyksessä on uusi tuote, on tilastotietoa vähän ja vakuuttamisen perusteet voivat muuttua vuosittain. Hänen oli myös vaikea nähdä, että kukaan vakuuttaisi itseään kybervakuutuksella. Haastateltava A nostaa esiin, että monilla yrityksillä on aineetonta pääomaa, mitä ei voi saada takaisin, jos ne tuhotaan. Jos maine menee tämän seurauksena niin miten maineriskin kykenisi hinnoittelemaan oikein. Esimerkiksi pankeilla maineriski näkyy siten, että asiakkaat lähtevät, kun jotain ikävää tapahtuu. Näin ollen pitäisi vakuuttaa myös sitä asiakas- ja pääomakatoa sekä osakekurssin pienentymistä.

Organisaatiolla B ei siis myöskään ollut kybervakuutusta. Haastateltava B:n mielestä hinta pitäisi olla aika alhainen, että he sitä ottaisivat. Ne vahingot mitä sattuvat ovat yksittäisiin koneisiin, jolloin uudelleen asennuksella saadaan ongelma poistettua. Haastateltava toi myöskin esille sen, että paljon parempi ratkaisu olisi pyrkiä varautumaan pahimpaan skenaarioon, ja laittaa vakuutuksen ostoon menevä rahasumma sen sijaan oman tietoturvan parantamiseen. Korvauksen väärtiä pohdittiin tilanteissa, joissa tappio on esimerkiksi maineeseen perustuva. Kybervakuutuksen mukana tulevien palveluiden konkreettista hyötyä punnittiin myös. Kybervakuutus tarjoaa siis muun muassa neuvontaa ja apua tietomurron paikannuksessa. Haastateltavan mukaan heidän organisaation IT-osasto pystyisi itse aika hyvin paikantamaan murron ja mitä tietoja on saatu varastettua. Mitä kykenevämpi organisaation IT-osasto on, sitä paremmin yritys pystyy itse selviytymään kyberhyökkäyksistä. Hän lisää, että jos kybervakuutuksesta jollain skenaariolla olisi hyötyä, voisi sen ottoa harkita, mutta päätöstä pitäisi kuitenkin punnita todella tarkkaan. Lisäksi ilmenneet ongelmat ovat usein sisäsyntyisiä, joten kysymykseksi nousi, kattaako kybervakuutus edes sellaisia, vai ovatko ne yrityksen omalla vastuulla.

Vakuutusyhtiöiden edustajilla on kuitenkin eri näkemys siitä, miten organisaatioiden IT-osasto pystyy vastaamaan tietomurtoihin. IT-osastot ovat tärkeässä asemassa, mutta kyberrikokset kuten esimerkiksi kiristystapaukset (ransomware) ovat aina ainutlaatuisia tapauksia, joita IT-osasto ei ole välttämättä koskaan aiemmin kohdannut. Tässä vaiheessa kyberriskeihin erikoistunut IT-konsultti on nopeampi ja osaavampi apu ja pystyy näin ollen pienentämään organisaatiolle mahdollisesti aiheutuvaa tappiota hyökkäyksestä johtuen.

Tutkimuksien mukaan kybervakuutustuotetta pidetään liian kalliina ja ylihinnoiteltuna. Haastateltava A:n mielestä vakuutusmaksut tulisivat varmasti ylittämään jopa vakuutettavien laitteiden ja asioiden summan, eikä näe siinä mielessä ideaa vakuutuksen ottamiseen. Haastateltava

D taas ilmaisee, että miten voi sanoa ylihinnoitelluksi, jos riskiä ei tiedetä. Vakuutusasiantuntijoiden näkemysten mukaan syitä ostamattomuuteen on osittain raha. Vakuutus on aina uusi menoerä, jolle ei välttämättä ole budjettia ja päätöksentekoprosessi on iso. Esimerkiksi pienillä yrityksillä vakuutusmyynti tapahtuu yleensä toimitusjohtajan kanssa, joka ei välttämättä tiedä yrityksen juridisia ja rahallisia riskejä, joten hänen on yleensä puhuttava monelle eri taholle ennen päätöksentekoa. Eri osastot voivat olla myös eri mieltä kannattaako vakuutusta ottaa vai ei ja päätösprosessi voi olla hyvinkin pitkä, jopa vuosia. Kybervakuutuksen myyntiprosessia käsitellään seuraavassa luvussa tarkemmin.

5.3 Kybervakuutusmarkkinat Suomessa

5.3.1 Kyberriskien ja -vakuutuksen tunnettuus sekä kohderyhmä

Vuonna 2015 Suomessa toimi yhteensä 55 kotimaista vakuutusyhtiötä. Näistä 38 oli vahinko- ja jälleenvakuutusyhtiöitä, 11 henkivakuutusyhtiöitä ja 6 työeläkeyhtiöitä. Yhtiöissä palveli yhteensä keskimäärin 9690 henkeä. Vuodesta 2014 määrä on laskenut 1190 hengellä, mikä johtuu LähiTapiolan henkilöstön uudelleen järjestelyistä. Vuonna 2015 Suomessa toimi 14 ulkomaalaisen vakuutusyhtiön edustustoa. Finanssivalvonnalle oli tämän lisäksi noin 680 ulkomaista yhtiötä tehnyt ilmoituksen vakuutuspalveluiden tarjoamisesta rajan yli. Yhtiöiden yhteenlaskettu vakuutusmaksutulo oli 2015 vuonna 45 miljardia euroa, joten se kasvoi 3 % edellisvuodesta. Vakuutusmeklariyrityksiä vuonna 2015 oli yhteensä 77. (www.finanssiala.fi)

Kolme suurinta vakuutusyhtiötä hallitsevat vahinkovakuutuksen markkinaosuuksia. OP-Pohjola-ryhmä 31,8 prosenttia, LähiTapiola-ryhmä 25,4 prosenttia sekä If-konserni 23,6 prosenttia. Vakuutusmarkkinoiden rakenteelle tyypillistä Suomessa on lakisääteisistä vakuutuksista kerättyjen maksujen suuri osuus koko alan maksutulosta. Vuonna 2015 maksutulosta 61 % saatiin lakisääteisistä vakuutuksista. Suomen vakuutusmarkkinat ovat myös vahvasti keskittyneet ja neljän suurimman henki-ja vahinkovakuutusyhtiön osuus maksutulosta oli 85 %. (www.finanssiala.fi)

Suomessa kybervakuutustuotteita tarjoavat OP-Pohjola Vakuutus, AIG sekä If. On tavanomaista, että vakuutusyhtiöt tekevät yhteistyötä IT- alan yrityksen kanssa kybervakuutuksen tarjoamisessa. OP-Pohjola Vakuutus tekee yhteistyötä teknologiayhtiö CGI kanssa. If taas tekee

yhteistyötä IBM teknologiayrityksen kanssa ja AIG vakuutusyhtiön kumppanina taas puolestaan on teknologiayhtiö Nixu Oy.

Haastatteluiden perusteella kybervakuutus on Suomessa yritysten keskuudessa vielä varsin tuntematon. Kumpikaan haastattelemistani yrityksistä ei ollut kuullut kyseenomaisesta vakuutuksesta ennen haastattelua. Haastateltava D esittää, että asiakas ei ole se asiantuntija ja näin ollen asiakkaalle lähdetäänkin tarjoamaan ratkaisuja. Organisaatio D tuotti asiakkaillaan tutkimuksen, jonka mukaan 50–60% yrityksistä pitää todennäköisenä, että heihin kohdistuu tietomurto. Vaikka yli puolet pitävät tietomurtoa todennäköisenä, vain 13 % sanoivat varautuneensa siihen. Näin ollen tietoisuuden riskeistä voi katsoa nousseen, mutta seuraava askel eli käytännön toiminta on vielä tekemättä. Haastateltava D kertoo, että enää ei tarvitse puhua yrityksille, että on olemassa tietynlaisia tietoturvariskejä, koska tietämys on niin hyvä. Kysymykseen tuleekin se relevanssi, että yritykset saavat yhdistettyä sen, mitä tämä riski heidän yritykselle tarkoittaa ja miten heidän yrityksen kannattaisi siihen varautua.

Kuitenkin kyberriskien ja -vakuutuksen tunnettuutta lisää koko ajan lisääntyvät kyberseminaarit ja tilaisuudet. Haastateltava C:n, E:n ja F:n mukaan isot asiakkaat ovat enemmän tietoisia niin tuotteesta kuin riskeistäkin, koska käyttävät vakuutusmeklareita, jotka kertovat riskeistä ja mahdollisista suojautumisvaihtoehdoista. Pienemmät yhtiöt ovat vähemmän tietoisia muun muassa juuri näiden syiden takia. Organisaatio F järjestää kyberriskiseminaareja ja pitääkin niitä hyvänä kanavana tiedottaa tuotteesta sekä riskeistä ja näin ollen seminaarit toimivat hyvänä kybervakuutuksen myynninedistämisenä. Tietoisuus on kuitenkin vielä huono, joskin se on kasvamassa koko ajan. Tietoisuus riskeistä ja relevanssi yksittäisten yritysten osalta on se missä tapahtuu koko ajan kehitystä. Monesti ei tiedetä mitä osa-alueita tuote sisältää ja mitkä olisivat ne tärkeimmät tuotteen osa-alueet itselle. Monesti kybervakuutus saatetaan myös sekoittaa joko omaisuus-, vastuu- tai rikosvakuutuksiin niiden osittain samankaltaisten korvauspiirien takia. Tuotteen huono tietämys nähdään kuitenkin vakuutusyhtiön ongelmana, jos he eivät kykene kunnolla selittämään tuotteitaan. IF vakuutusyhtiölle tietoturvavakuutus on tullut asiakkaiden tarpeiden johdosta. Vakuutusyhtiön perusajatus on tarjota turvaa asiakkailleen, ja uusien riskien ilmaantuessa, on vakuutusyhtiön tehtävä vastata näihin riskeihin.

Näkemykset siitä, ketkä ostavat kybervakuutuksen ja ovat näin kybervakuutuksen asiakaskuntaa, erosivat hiukan haastateltavien keskuudessa. Haastateltava C kommentoi, että kaikki yritykset niin isot sekä pienet ostavat kybervakuutuksen. Suomen top 10 yrityksistä osa saattaa

ostaa ja osa ei riippuen siitä, miten yritykset näkevät ja havaitsevat riskin. Jos on vähittäiskaupan alalla toimiva yritys, ei varmaan osta kybervakuutusta, koska liiketoiminnan keskeytysriski ei ole niin suuri, koska tuotteita voi myydä eri tavoilla. Asia on toinen, jos olet tuottaja tai tehdas yritys, jolloin riski on paljon suurempi. Haastateltavat E ja F mieltävät, että suuret yritykset ostava ensin ja usein siihen vaikuttaa se, että välissä toimii meklari, jonka kautta riski nousee ylös. Myös suurilla yrityksillä, joilla on meklari, on ylipäätään huolehdittu paremmin riskienhallinnasta ja heillä on myös varaa ostaa kybervakuutus muiden vakuutuksien lisäksi.

Osa vakuutusyhtiöistä siis tarjoaa kybervakuutusta vain suurimmille yrityksille, kun osa taas tarjoaa sitä kaikenkokoisille. AIG ja OP Pohjola tarjoavat tuotetta vain suuryritysasiakkaille. Haastateltava E kertoo, että AIG targetoi niitä yrityksiä, joilla on maksukykyä ja joissa raha liikkuu, eli suuryrityksiä. Heidän ansaintalogiikkansa on myös se, että yhdestä isosta yhtiöstä voi saada saman verran rahaa kuin 10 pienestä, mutta vähemmällä vaivalla, joten siksi pieniä yhtiöitä ei käydä läpi. Siihen ei myöskään ajallisesti olisi resursseja. OP Pohjola taas on suunnitellut kybervakuutustuotteen suuryritysasiakkaille kysynnän perusteella eli kohderyhmäksi on valikoitunut se, josta kysyntä tulee. IF tarjoaa vakuutusta myös pienille sekä keskisuurille yrityksille, joten heidän lähestymistapa tuotteeseen on hieman erilainen. Haastateltava D:

”Onko sinulla sellaista tietoa, joka on sinulle tai asiakkaalle arvokasta? Aika harva sanoo ei. Ja oletko yhteydessä verkkoon? Kyllä tai ei. Tää kertoo siitä riskistä, josta puhutaan. Periaatteessa kaikki yritykset ovat kohderyhmää. ”

Kysymykseen tulee se, kuinka suuri riski kullekin yritykselle on ja se, miten yritykset katsovat riskiä toimialasta riippuen. Tietomurron aiheuttama liiketoiminnan keskeytyminen on internetkaupalle merkittävä riski, kun taas esimerkiksi asiantuntijaorganisaatioilla, joilla on paljon arvokasta tietoa, on erittäin tärkeää näiden tietojen suojaaminen ja palauttaminen. Haastateltava C:n mielestä suuremmassa vaarassa ovat pienet yritykset, koska ne ovat helppo kohde. Miksi joku yrittäisi hakkeroida pankin IT-järjestelmiin ja varastaa 5 miljoonaa euroa ja tämä kestäisi 2 vuotta, kun puolessa tunnissa voisi hakkeroida pieneen yritykseen Rovaniemeltä ja varastaa 20 000 euroa. Pienet yritykset myös usein ajattelevat, etteivät ole kyberrikoksien kohteena, juuri sen takia että ovat pieniä yrityksiä.

Kiinteistöihin ja niiden järjestelmiin liittyvät riskit ovat lisääntymässä. Suomessakin on ollut hyökkäyksiä jäähalleihin, jossa aiheutetaan jään sulaminen, joten kyseessä on aivan erilainen riski. Asiakkaiden tarpeet tietomurtoihin liittyen ovat siis hyvinkin erilaisia. Pienet yritykset arvostavat palveluja joita kybervakuutuksen mukana tulee. 24 tuntia vuorokaudesta saatavissa

oleva apu vahinkotilanteissa on olennainen osa palvelupakettia ja se osaaminen, miten saadaan tiedot rakennettua takaisin ja liiketoiminta taas ylös kyberriskin toteutuessa. Isoilla yrityksillä voi taas korostua liiketoiminnan keskeytymisestä aiheutuva taloudellinen vahinko sekä vastuukysymykset.

Haastateltava B:n mielestä kybervakuutusta ei ole järkevää tarjota kuin pienille firmoille, joilla ei ole kunnon IT-osastoa ja sen puolesta IT-osaaminen on heikompaa. Tällaisessa tapauksessa vakuutuksen avulla saataisiin lisää osaamista ja palveluita, jotka tulisivat yrityksen itse hankkimina paljon kalliimmiksi ja näin ollen vakuutuksen osto toisi selkeää lisäarvoa yrityksille riskin sattuessa. Haastateltava A taas oli sitä mieltä, että vakuutusta ei ole juurikaan järkeä tarjota muille kuin isoille yrityksille, koska pienimmillä tuskin olisi varaa siihen.

Kun isoimmissa yrityksissä riskienhallinta ammattilaiset lähtevät analysoimaan, kannattaako vakuutus ottaa vai ei, he nojaavat riskienhallinnan perus vaihtoehtoihin, jotka ovat siirrä, hyväksy, pienennä ja poista. Tämä prosessi liittyy pääoman allokointiin ja voi olla, että riskiä ei voida poistaa, mutta sitä vähennetään. Aina jää jäännösriski, jota pitää osata arvioida, kannattaako se siirtää vai hyväksyä, ja tämä liittyy vakuutuksen ostopäätöksen tekemiseen. Yritykset voivat päätyä tulokseen, että tämä ei tällaisenaan ole järkevä riskienhallinnan keino meille. He voivat myös ajatella, että ovat varautuneet tilanteeseen niin paljon jo muilla keinoilla, ettei vakuutus ole enää kannattava.

Haastateltava F painottaa, että kohderyhmää ovat ne yritykset, joista kysyntä tulee. Tällä hetkellä suuryritykset ja teollisuus ovat eniten kiinnostuneita juuri keskeytysriskin takia. Esimerkiksi, jos tehdas hakkeroidaan se on sama asia kuin että tehdas palaa, luultavasti kesto on lyhyempi, mutta siltä ajalta sama keskeytysvahinko. Ongelmallisina aloina hän näkee muun muassa energiantuotannon sekä tietynlaiset maksujenvälittäjät. Normaalisti vakuutusmäärät ovat olleet kybervakuutuksessa aika pieniä ja jos voimantuotanto esimerkiksi pysäytetään, keskeytysvahinko menee läpi vakuutusmäärän todella nopeasti. Haastateltava E taas kertoo, että terveydenhoitoala sekä finanssiala ovat suurimpia heidän asiakkaitaan, koska heillä on paljon henkilötiedoista aiheutuvaa riskiä. Eri alat katsovat myös riskiä eri näkökulmista. Teollisuusala katsoo riskiä siltä näkökulmalta, että mitä heille itselleen voi aiheutua, kun taas finanssiala katsoo mitä vaatimuksia heille voi tulla riskin toteutuessa sekä mahdollinen maineen menetys.

Haastateltava F näkee myös terveydenhoitoalan kiinnostavana, mutta ongelmana on se, että suurin osa siitä on julkisella puolella, jolloin vakuutus olisi julkinen hankinta. Julkisella puolella budjetit ovat olleet monta vuotta tiukoilla, ja näin ollen vakuutuksen myyminen on hankalaa käytännön syistä.

Haastateltava D:n kokemuksen mukaan voidaan sanoa kaksi syytä, miksei vakuutusta osteta. Ensimmäinen on se, että ei ehkä tiedetä, että on mahdollisuus siirtää tämän tyyppisiä riskejä vakuutusyhtiön kannettavaksi. Toinen on se, että hyväksytään riski, joka ei perustukaan järkevään analyysiin. Usein myös uskotaan, että ei se meille satu tai sitten jos sattuu, niin ei se paljoa maksa. Asian suhteen voidaan olla välinpitämättömiä eikä koko asiaa haluta miettiä. Kun ei mietitä ei myöskään tehdä analyysiä ja silloin saatetaan katsoa vain sitä euromäärää, mitä vakuutus maksaa. Uuden tuotteen kohdalla myös ajatellaan, että tämä on lisäkustannus. Osittain vakuutus jää myös ostamatta juuri rahan takia, koska kyseessä on uusi menoerä. Vakuutus on myös aina vaihtoehtoiskustannus. Hänen mielestään yritysten pitäisi pystyä ajattelemaan, että tällä katetaan nyt riskejä, joita aikaisemmin ei pystytty vakuutuksella kattamaan.

Haastateltava C nostaa esiin, että esteenä vakuutuksen ostoon on osittain myös se, että asiakkailta vaaditaan liian paljon informaatiota heidän tietosuojan tasostaan. Haastateltavien E ja F mukaan organisaatioiden omat IT-osastot ovat niitä, jotka eniten vastustavat kybervakuutuksen ostoa. Tämä saattaakin alkuun vaikuttaa erikoiselta, mutta syy on yleensä se, että it-ihmiset yrityksissä kokevat yleensä, että kybervakuutus on turha ja epäluottamuslause tietoturvaosastolle. Riskienhallinnan osasto taas usein ostaa vakuutukset, mutta kyberriskejä ei nähdä samalla tavalla fyysisenä riskinä ja näin ollen he voivat mieltää sen IT-osastolle kuuluvaksi. Vastuuriskit taas kuuluvat enemmän lakipuolelle ja maineasiat viestinnälle. Haasteena on se, että kyber yhdistää näistä kaikista osia, mikä johtaa siihen, että ei tiedetä kenen pitäisi päättää tästä asiasta ja kenen maksaa. Haastateltava C:n kokemuksen mukaan myös päätösprosessi organisaatiossa on usein monivaiheinen ja pitää sisällään useita eri ihmisiä, joilla on erilaiset mielipiteet asiasta. Esimerkiksi pienten yritysten kanssa asioidessa myynti tapahtuu yleensä toimitusjohtajan kanssa, joka ei välttämättä tiedä rahallisia ja laillisia riskejä, joten hänen on puhuttava ensin eri osastojen asiantuntijoille ennen ostopäätöksen tekemistä.

Haastateltavat C ja F kertovat, että suomalaisilla yrityksillä on tapana vertailla itseään toisiinsa. Jos naapurilla ei ole kybervakuutusta ei sitä varmasti meilläkään tarvitse olla. Helposti myös ajatellaan, että Suomi on niin sanotusti syrjässä kaikelta ja markkina on niin pieni, että ongelma ei ole samalla tavalla meidän kuin muualla maailmassa. Haastateltava F kiteyttää:

"Ajatellaan, et tämä on aika helppoakin. Sulle tulee sähköposti, joka on kirjoitettu huonolla suomen kielellä, kaikki näkee et tämä on huijausta, mut nämä modernit kohdennetut hyökkäykset ovat jotakin ihan muuta ja Suomen pitäisi varautua paljon paremmin. "

Suuryrityksistä puhuttaessa edelläkävijät Suomessa ovat jo hankkineet kyberturvaa muutamia vuosia sitten. Enemmän ehkä kokeilumielessä, mutta mitä enemmän mietitään missä riskejä on ja miten ne vaikuttavat omaan yhtiöön, niin sitä suurempia vakuutusmääriä otetaan. Haastateltavien E ja F mukaan keskeytysriski on se riski, joka myy kybervakuutuksia tällä hetkellä.

5.3.2 Myyntiprosessi

Kybervakuutuksen myyntiprosessi vaihtelee yrityksen koon mukaan. Organisaatio D haluaa viedä tuotteesta turhaa mystiikkaa pois ja haluaakin tehdä oston mahdollisimman helpoksi kaiken kokoisille yrityksille. He eivät myöskään tee kyberturvallisuusanalyysiä pienimmille yrityksille, ja tällä vakuutuksenotto halutaan tehdä vieläkin helpommaksi. Riskiä pystytään hallitsemaan pienimmillä yrityksillä ilman kyberturvallisuusanalyysiäkin. Isoimmilla yhtiöillä tehdään kyberturvallisuusanalyysi ja silloin riskitkin ovat usein haastavampia. On myös asiakkaan etu, että analyysi tehdään. Suuryritysten kanssa käydään tekniset ratkaisut läpi, mitä taloudellisia vahinkoja tulee, jos tietyt skenaariot toteutuvat, jolloin asiaan tulee analyyttinen lähestymistapa. Lisäksi arvioidaan esimerkiksi IT-arkkitehtuuri ja katsotaan, onko ulkoisia palveluntarjoajia ja mikä on tietoturvan taso. Sitten katsotaan mitä vakuutus voisi kattaa ja lähdetään miettimään vakuutuksen sisältöä, omavastuuosuuksia sekä -aikoja. He aikovat tuoda kybervakuutuksen nettiin vielä tänä vuonna, jolloin sen ottamiseen ei mene välttämättä kuin 10 minuuttia. Muualla pohjoismaissa IF vakuutusyhtiön kybervakuutuksen voi jo ostaa netistä.

AIG vakuutusyhtiön myyntiprosessi on muuttunut tuotteen myymisen aloittamisesta. Ennen tehtiin niin kutsuttuja työpajoja, jotka osoittautuivat kuitenkin liian raskaiksi ja tällä hetkellä asiakas täyttää kyselykaavakkeen ennen vakuutuksen myyntiä. Lisäksi yrityksen nettisivujen IP-osoitteesta tehdään raportti ja katsotaan, kuinka paljon hyökkäyksiä on tullut sivustolle. Myös jatkuvuussuunnitelma ja eri sopimusehtoja pyydetään nähtäville. Näillä toimilla haetaan organisaation kypsyysastetta. Keskimääräinen myyntiaika tällä hetkellä on 3-6 kuukautta ja suurimpana myyntikanavana toimivat meklarit. AIG:n kybervakuutusta ei voi ostaa netistä, koska riskienkartoitus on vielä sellaista, että ihmisen on käytävä analyysista saadut tulokset

läpi. Joskus, jos heille tulee kybervakuutus pienimmille yrityksille, netistä ostaminen voisi hänen mukaansa olla mahdollista.

OP Pohjola käyttää kysymyspatteristoa välineenä kartoittaa suuryritysasiakkaiden yrityksen tietoturvan tilaa. Haastateltava F:

”Aika monella vakuutusyhtiöllä käynyt tässä kybervakuutuksen alkutaipaleella niin, että kun ovat lähteneet tutkimaan asiaa ja luovuttaneet raportin, että teidän pitää tehdä nämä ja nämä asiat ja sitten asiat ovat kunnossa niin asiakas ilmoittaa, kiitos tästä ilmaisesta raportista nythän ei tarvita enää mitään kybervakuutusta, kun asiat ovat kunnossa. "

Pienille yhtiöille on hänen mukaan turha lähteä isoja asioita selvittelemään ja hän ei näekään tätä riskin hallinnoimiskeinona vaan vakuutustoiminnan ydinperiaatteen eli tarpeeksi suuren vakuutuskannan, joka kestää yksittäiset vahingot. Jos myynnistä tekee liian hankalaa, kukaan ei osta tuotetta. OP Pohjola on lanseeraamassa kybervakuutustuotetta myös pienille ja keskisuurille asiakkaille ja tarkoitus on, että tämä tuote on ostettavissa myös netistä. Asiakkaan on aivan aluksi miellettävä, että hän on ylipäätään riskillä. Haastateltavan mielestä se, että yritykset ovat riskillä, ei ole mikään uusi asia. Sen jälkeen yrityksen on suhteutettava sitä omiin toimintoihin, eli jos riski tapahtuu, kuinka suuri osa esimerkiksi liikevaihdosta häviää. Tämän jälkeen on päätettävä, kenen budjetista kybervakuutusmaksu menee.

Haastateltava C kuulee myynnissä usein kysymyksen "Ovatko toiset suomalaiset yritykset ostaneet kybervakuutuksen?", mikä on hänen mielestään outoa. Niin kuin on sanottu Suomalaiset yritykset vertailevat itseään helposti muihin suomalaisiin yrityksiin, vaikka toimisivatkin globaalisti. Ongelmana tässä on se, että Suomessa tietyillä toimialoilla ei ole montakaan vastaavanlaista yritystä joihin omaa yhtiötä voisi vertailla. Hyvänä esimerkkinä tästä toimii Neste. Hän näkee tuotteen myymisen helpottuvan kuitenkin koko ajan. Heidän asiakasmäärä on kolminkertaistunut vuodesta 2015 vuoteen 2016, joten vuosi 2017 näyttää lupaavalta. Mitä useammat vakuutusyhtiöt alkavat tarjota tuotetta, sitä helpommaksi myös vakuutusmeklari yritysten asema kybervakuutuksen myynnissä muuttuu. Myyntiprosessi on heillä pitkä ja voi kestää vuodenkin. Yleensä asiakas tavataan 3-4 kertaa ja tämän aikavälin pituus vaihtelee täysin asiakkaasta riippuen. Myös muut haastateltavat näkevät myyntiprosessin suuryritysasiakkaille pitkänä jopa yli vuoden mittaisena.

5.3.3 Kilpailu Suomen kybervakuutusmarkkinoilla

Suomen kybervakuutusmarkkinoille on ehtinyt syntyä jo kilpailua, vaikka tuote on ollut Suomalaisten tarjoamana markkinoilla vain 1,5 vuotta ja ulkomaalaisten tarjoamana 3-4 vuotta. Vakuutusyhtiöiden asiantuntijoiden mukaan kilpailu kiristyy ja tarjonta kasvaa jatkuvasti. Suuryritysten osalta varsinkin kilpailu on tiukkaa, kun yritykset haluavat kattavia ratkaisuja edulliseen hintaan, kun taas pienemmillä toimialoilla ratkaisu voi olla enemmän standardi. Haastateltava D painottaa, että hekin varautuvat kovempaan kilpailuun ja miettivät, mikä on se heidän juttu millä erottaudutaan kilpailijoista.

Kaikkien haastateltavien mukaan Suomen kybervakuutusmarkkinoilla on hyvin paljon kilpailua. Kilpailua ei ole niinkään vielä suomalaisten yhtiöiden kesken vaan se on lähinnä ulkomaalaisten yhtiöiden hallussa. Monet ulkomaalaiset vakuutusyhtiöt yrittävät kybervakuutustuotteen avulla päästä kiinni myös muihin omaisuuslajein Suomen vakuutusmarkkinoilla. Kaikilla ei siis itsessään ole välttämättä intressiä kybervakuuttamiseen vaan sen avulla yritetään hankkia lisää asiakkaita ja saada kysyntää myös muille vakuutusyhtiön vakuutustuotteille Suomen markkinoilla.

Kun mietitään, millainen osa Suomen vakuutusmarkkinoita kybervakuutus on, niin vastaus on pieni, kun läheskään kaikilla vakuutusyhtiöillä ei ole tarjoamassaan tuotetta. Myöskään kaikille asiakassegmenteille ei tuotetta kaikki, joilla se on, tarjoa. Suurin osa vakuutusmarkkinoista on myöskin yksityishenkilöiden vakuutusmaksua ja koska kybervakuutus on yritysten ratkaisu, on kybervakuutus myös niin maksutulossa kuin kapasiteetissakin pieni. Haastateltava C esittää, että on vaikea sanoa paljon kybervakuutus olisi vakuutusmaksutulossa Suomessa, mutta arviolta 1-1,5 miljoonaa.

Haastateltava D:n mielestä kasvunopeus tulee kuitenkin olemaan todella nopea. Haastateltava C taas lisää, että uusien toimijoiden on hankala tulla markkinoille, koska heillä ei ole dataa eikä kokemusta tuotteesta, jolloin heidän vakuutustuotteen hinta on yleensä korkeampi kuin muiden jo markkinoilla olleiden. Tämä taas johtaa siihen, että uusien tulokkaiden on hankala lähteä hintakilpailuun mukaan.

Kybervakuutusmarkkinat ovat tällä hetkellä pehmeät ja hinnat ovat hyvin edulliset pohjoismaissa verrattuna muihin maihin. Hintojen alhaisuus selittyy sillä, että kyseessä on uusi tuote jossa ei ole tapahtunut vielä paljoa vahinkokehitystä. Kun vahinkoja alkaa sattumaan enemmän

se tulee näkymään myös hinnoissa. Hinnoissa on myös oltava varmuuslisää, mutta tästä huolimatta hintoja pohjoismaissa pidetään todella alhaisina tällä hetkellä. Haastateltava F arvioi, että kunhan markkina kasvaa ja vahinkoja alkaa tulla, hinnat vakiintuvat ja näin ulkomaalaiset yhtiöt eivät pysty polkemaan hintoja alas, jolloin OP Pohjolankin markkinaosuus tulee kasvamaan. Kaikkien vakuutusyhtiöiden mukaan kybervakuutuksen osuus heidän liiketoiminnastaan oli vain muutamia prosentteja, mutta kasvutavoitteita vuodelle 2017 on asetettu.

Vakuutusyhtiöiden edustajat näkivät poikkeuksetta kaikki kybervakuutuksen tulevaisuuden hyvänä. Haastateltava C toteaa, että vakuutustuotteet ovat olleet markkinoilla jo jonkin aikaa ja ne ovat kehittyneet ja standardisoituneet ja tulleet paljon ymmärrettävämmiksi ja tarjoavat suojaa riskeiltä joita asiakkaat kohtaavat. Datan kasvamisen myötä hinnoittelusta on myös tullut helpompaa. Molempien osapuolien, vakuutuksenottajien kuin -antajien, nähdään olevan enemmän koulutettuja kyseenomaisesta riskistä. Kyberturvallisuusseminaarit ovat yleistyneet ja keräävät paljon kuulijoita. Myös markkinoille tulleiden uusien suomalaisten vakuutusyhtiöiden myötä kybervakuutuksen myynti on muuttunut helpommaksi muun muassa meklareille, koska monet suomalaiset yritykset haluavat ostaa vakuutuksensa suomalaisesta vakuutusyhtiöstä. Mitä enemmän toimijoita on markkinoilla, sitä tunnetummaksi tuote tulee. Haastateltava E arvioi, että turva tulee tulevaisuudessa muuttumaan ja jatkossa tulee olemaan erilaisia turvatasoja, joissa ei ole kaikissa niin kattavaa suojaa.

Vuonna 2018 voimaan astuvan uuden Euroopan Unionin tietosuojalainsäädännön nähdään lisäävän kybervakuutuksen myyntiä. Haastateltava D:n mukaan uusi lainsäädäntö tuo nimenomaan enemmän relevanssia ja konkretiaa kyberriskeihin. Se tuo mukanaan myös velvollisuuden ilmoittaa tietosuojavaltuutetulle tietyin edellytyksin ja nopealla aikavälillä sattuneista kyberhyökkäyksistä. Kysymykseen tulee siis, haluaako yritys olla omalla vastuulla vai vakuutuksen. Haastateltava F mieltääkin oudoksi sen, että yritykset ajattelevat, että silloin kun uusi lainsäädäntö astuu voimaan pitää asioiden olla kunnossa. Yritykset ovat kuitenkin jo nyt riskillä ja heidän maine voi jo mennä kyberriskin toteutuessa. Maineen menetys voi olla paljon suurempi tappio kuin tietomurron seurauksena saadut sakot.

5.3.4 Yhteistyö IT-organisaatioiden kanssa

Kybervakuutukselle on ominaista, että vakuutusyhtiöt tekevät yhteistyötä IT-alan toimijan kanssa. Haastateltavat ovat yhtä mieltä siitä, että tässä yhteistyössä on nähtävissä niin positiivisia kuin negatiivisiakin puolia.

Haastateltava C:n kokemuksen mukaan yhteistyön negatiiviset puolet saattavat tulla esiin isojen yrityksien kanssa, jotka tekevät yhteistyötä esimerkiksi konsulttiyrityksien kanssa. Isot yhtiöt haluavat usein käyttää omia palveluntarjoajia, jotka tuntevat heidän liiketoimintansa kuin vakuutusyhtiön kanssa yhteistyötä tekevää IT- yhtiötä, joka ei tunne heidän liiketoimintaansa niin hyvin. Yritykset voivat nähdä sen myös jopa loukkaavana kun vakuutuksen myötä he ovat niin sanotusti pakotettuja käyttämään vakuutusyhtiön kanssa yhteistyötä tekevää IT-yhtiötä, jos riski toteutuu. AIG on juuri tästä johtuvasta syystä muuttanut tuotettaan niin, että asiakas voi halutessaan valita eri palveluntarjoajan kuin heidän kumppaninsa. Heidän kybervakuutustuotteen rakenne on suunniteltu uudestaan, ja tämä IT-palvelu toimii nyt lisäosana, jonka voi halutessaan ostaa tai olla ostamatta, ettei kukaan koe maksavansa turhasta.

Haastateltava F:n mielestä vakuutusyhtiön on pystyttävä jollain tasolla seuraamaan mitä tapahtuu, jonka takia heillä ei ole asiakasyrityksen mahdollista käyttää omaa palveluntarjoajaa. Haittapuolina kumppaneiden käytössä hän näkee sen, että jos kumppanit saavat rahaa siinä suhteessa paljonko tekevät, he haluavat tehdä mahdollisimman paljon. Myös riskit kasvavat, kun vakuutusyhtiö lähtee koordinoimaan tällaista palvelupalettia ja, jos sitä ei hoida oikein niin riskihän on, että aiheuttaa asiakkaalle vahinkoa. Monet tietoturvayhtiöt eivät myöskään ole nähneet kybervakuutusta itsessään kiinnostavana vaan tapana päästä laskuttamaan joko vakuutusyhtiötä tai asiakasta eli pääsemään kiinni uusiin asiakkaisiin.

Pienille yrityksille vakuutusyhtiön yhteistyö IT-yhtiöiden kanssa voi olla erinomainen etu, koska näin he saavat yhteyden palveluihin matalammilla kustannuksilla kuin jos he ostaisivat palvelut suoraan IT-yritykseltä. Tietoturvakonsulttien laskutukset ovat suuria ja pienenkin tietomurron selvittäminen kestää helposti 10 tuntia ja lasku on sen mukainen. Vakuutuksessa kulu rajataan omavastuuseen ja vakuutusyhtiöiden tekemä sopimus on varmasti asiakkaalle edullisempi.

Globaalista IT-kumppanista on vakuutusyhtiöiden mukaan myös se hyöty, että ne eivät koskaan nuku, sillä koskaan ei tiedä mistä asiakkaaseen kohdistuvassa tietomurrossa on kyse ja mistä päin maailmaa hyökkäys tulee. Vahinkotilanteen haltuunotossa on näin ollen paljon apua IT-

kumppanista. Kumppanit osaavat kertoa asiakkaan tietoturvan tason, määritellä minkä tyyppisiä palveluita erilaiset asiakkaat tarvitsevat sekä ottaa vahingon hallintaa, kun se tapahtuu. Hinnoittelu, riskinvalinta sekä vakuutuksen myöntäminen ovat tietenkin vakuutusyhtiön vastuulla.

5.3.5 Haitallinen vakikoituminen, moraalikato sekä jälleenvakuuttaminen

Kuten vakuutuksen luonteeseen kuuluu, myös kybervakuutuksessa tulee esiin haitallinen valikoituminen sekä moraalikadon ongelmat. Haastateltavien mukaan haitallista valikoitumista ja moraalikatoa hallitaan paljon vakuutusehdoilla. Haastateltava D kertoo esimerkin, jossa tapasi asiakkaan, joka halusi vakuuttaa vanhan IT-järjestelmän. Asiakas ei kuitenkaan aikonut huoltaa järjestelmää ja he kysyivätkin, onko se vakuutettu, jos järjestelmä kuolee. Vastaus tähän on, että tietenkään ei, eli vakuutus vaatii, että kaikki päivitykset ja huollot tehdään.

Jos asiakkaalla on ollut tietomurto aikaisemmin, on todennäköistä, että he ostavat vakuutuksen. On myös melko todennäköistä, että he ovat panostaneet enemmän tietoturvaan tämän tapahtuman jälkeen. Jos asiakkaalla on kybervakuutus ja tietomurto tapahtuu, nousee yleensä myös vakuutusmaksu.

Haastateltavien mukaan Suomalaiset yritykset ovat lähtökohtaisesti todella rehellisiä. Haastateltava D:n mielestä vaarana on se, että ajatellaan että vakuutus on se tietoturvan riskienhallintamuoto eikä se, että lähdetään vertaamaan tietoturvapalveluiden ja vakuutuksen hintaa. Tämä on haaste, mutta sitäkään ei ole vielä paljoa huomattu tapahtuvan. Toinen haaste on se, että yritykselle on ehkä sattunut aikaisemmin joku kyberhyökkäys ja tästä huomataan, että on olemassa joku tietynlainen riski joka tulisi todella kalliiksi ja tähän otetaan vakuutus. Kun on kyse vielä uudesta tuotteesta moraalikadon ja haitallisen valikoitumisenkin ulottuvuudet muotoutuvat vielä.

Haastateltava E:n kokemuksen mukaan ei ole näkynyt juurikaan haitallista valikoitumista, koska vakuutus on sen verran hintava, joten puhutaan vain yksittäisistä tapauksista. Esimerkiksi yritys voi juuri ajatella pelkän vakuutuksen riittävän kyberriskeihin varautumiskeinona. Vakuutusyhtiö ei myöskään lähde myyntiprosessiin mukaan, ellei yrityksen riskienhallinta ole kunnossa. On myös tietoturvapalveluita tarjoavia asiakkaita, jotka tietävät riskit erittäin hyvin. Vakuutusyhtiön vastuulla on hinnoitella näitä riskejä oikein.

Jälleenvakuuttamisen rooli Suomen kybervakuutusmarkkinoiden yhtenä osa-alueena on merkittävä. Jos vakuutusyhtiö toimii muuallakin kuin vain Suomen markkinoilla voi neuvottelutilanne jälleenvakuuttajien kanssa olla parempi. Haastateltava D kertoo, että heillä on uniikki tilanne, koska pohjoismaalaisena yhtiönä he voivat kantaa riskiä enemmän, joten isommankin vahingon sattuessa laiva ei heti uppoa.

Jälleenvakuutuksen avulla nostetaan kapasiteettia ja näin saadaan suurempia korvaussummia ja suurempi vakuutussuoja yrityksille. Suuri kapasiteetti on tämän kaltaisissa riskeissä todella tärkeä, koska jos on iso yritys, jonka koko liiketoiminta on verkossa ja tapahtuu kyberhyökkäys, vakuutusyhtiöt tarvitsevat biljoonia kapasiteettia, jotta voivat vakuuttaa tällaisen liiketoiminnan keskeytysriskin. Haastateltava A ihmetteleekin, että vakuutusyhtiöt ovat lähteneet liikkeeseen todella isolla riskillä, koska mitään kuvaa riskin suuruudesta ja sen kehittymisestä ei voi olla.

Jälleenvakuutus on todella isossa roolissa varsinkin kybervakuutuksessa, koska riski on todella suuri ja dataa on vähän. Haastateltava F kommentoi, että jälleenvakuutusta hankitaan kumulaatioriskeille ja oikeasti massiivisille riskeille. Jos esimerkiksi 100 000 miljoonan riski toteutuisi yhtäkkiä, se tekisi isoa tappiota vakuutusyhtiön tulokselle. Jälleenvakuutusmarkkinat voivat myös rajoittaa ensivakuutusmarkkinoiden tuotteita, jos niiden takana ei ole tarpeeksi kattavaa jälleenvakuutusta. Jos vakuutusyhtiö on myös liian sitoutunut ja riippuvainen jälleenvakuuttajasta, se ei enää kontrolloi omaa tuotettaan, jolloin siitä tulee käytännössä jälleenvakuuttajan tuote.

6 JOHTOPÄÄTÖKSET JA YHTEENVETO

Tässä luvussa esitellään tutkimuksen johtopäätökset ja yhteenveto. Aluksi vastataan tutkimusongelmiin mahdollisimman kattavasti ja tuodaan esiin merkittävimmät tutkimustulokset sekä johtopäätelmät. Tässä haastatteluista saatua tietoa peilataan teoreettiseen viitekehykseen, jolloin päätelmät joko vahvistavat teoriaa tai tuovat uusia näkökulmia siihen. Lopuksi kappaleessa arvioidaan tutkimuksen luotettavuutta sekä pohditaan jatkotutkimusehdotuksia.

6.1 Tutkimusongelmiin vastaaminen

Tämän tutkimuksen tarkoituksena oli löytää vastaukset kahteen tutkimusongelmaan. 1) Miten suomalaiset yritykset ovat varautuneet kyberriskeihin? sekä 2) Millaiset ovat Suomen kybervakuutusmarkkinat vuonna 2016? Kyberriskit ovat polttava aihe tänä päivänä liiketoimintamaailmassa. Ammattikorkeakouluissa on jopa perustettu aivan omia linjoja kyberriskiosaaminen lisäämiseksi. Kyberriskit ovat jatkuvasti lisääntymässä samalla kun ne muuttavat muotoaan. Kaikki haastateltavat olivat samaa mieltä siitä, että suuremmat yritykset ovat tiedostaneet riskit sekä suojautuneet niiltä pieniä yrityksiä paremmin. Syyksi voidaan sanoa se, että isoilla on oma IT-osasto ja ne käyttävät myös vakuutusmeklareita, jolloin riskitietoisuus on paremmalla tasolla. Pienillä yrityksillä tietoisuus on huonompaa ja he eivät koe olevansa kyberrikollisten kohteena samalla tavalla, kuin isot yhtiöt. Aikaisemmissa tutkimuksissa isoimmiksi syiksi, jotka estävät yhtiöitä suojautumaan paremmin kyberriskejä vastaan on listattu tiedon ja osaamisen puutteen, vaikeuden arvioida riskin rahallista arvoa sekä budjettiin liittyvät rajoitteet. Nämä samat asiat tulivat ilmi myös haastatteluista. Kyberriski on uusi riski ja uusi menoerä oli se sitten vakuutuksen muodossa tai lisääntyneenä panostuksena tietoturvaan. Kyber vaatii myös erityisosaamista, mitä harvasta yrityksestä löytyy, jolloin riskiin ei osata varautua, jos ei siitä tiedetä kunnolla. Tietoisuuden nähdään lisääntyvän kuitenkin koko ajan muun muassa kyberturvallisuusseminaarien ja muun tiedottamisen sekä yhä enemmän sattuneiden kyberrikosten myötä.

Kyberriskeiltä yrityksissä on pyritty suojautumaan hyvin. Perus tietoturvaan panostaminen sekä henkilöstön koulutus kyberturvallisuusasioissa nähdään erittäin tärkeänä. Tutkimusten mukaan käyttäjien tietoisuus onkin tärkeässä roolissa kyberrikosten ehkäisyissä varsinkin verkkourkinta tapauksissa. Yritykset myös kertoivat, että ovat joutuneet jo muuttamaan toimintatapojaan lisääntyneen uhkan takia kuten muun muassa jakamaan riskiä siirtämällä ohjelmia eri palvelimille. Yritykset pitävätkin tärkeänä osana kyberriskeiltä suojautumista sitä, että koko henkilöstöllä on käsitys kyberturvasta ja hallitus sekä johtoryhmä ovat asiasta hyvin perillä. Kyberturvallisuus ei onnistu pelkällä IT-osaston työllä vaan yhteistyötä vaaditaan monien eri organisaation osastojen kanssa. Näin koko vastuu kyberriskeistä ei jää vain IT-osaston harteille. Yritykset näkevät kyberriskienhallinnan osana kokonaisvaltaista riskienhallintaa yhä enenevissä määrin, mikä on riskin hallitsemisen kannalta välttämätöntä. Yritykset myös mieltävät kyberriskin osittain tärkeämpään asemaan, kuin muut riskit, koska sen kanssa pitää jatkuvasti olla valmiudessa

ja kyberturva ei voi koskaan olla täysin kunnossa. Tämä vahvistaa aiempia tutkimuksia, joiden mukaan kyberriski on nostanut asemiaan top 10 riskeihin viimeisen kahden vuoden aikana. Tutkimuksien mukaan kyberriski onkin aliarvioiduin riski, jonka yritykset kohtaavat.

Kyberriskeissä on nähtävissä erilaisia trendejä ja tällä hetkellä kiristysohjelmat ja kohdennetut hyökkäykset ovat yleistyneet paljon. Kyberturvallisuutta onkin päivitettävä jatkuvasti, koska hyökkäystrendien mukaan riski muuttaa muotoaan. Näistä voidaan päätellä, että yritykset tiedostavat kyberriskien monimuotoisuuden ja laajuuden sekä sen, että riskiä on jaettava yrityksen sisällä, jotta siihen pystytään vastaamaan sen edellyttämällä tavalla. Tämän tutkimuksen valossa näyttäisi siltä, että yritykset ovat tiedostaneet riskin vakavuuden perusteellisesti ja riskiin on varauduttu hyvin. Kybervakuutusta ei kuitenkaan olla koettu tarpeellisena kyberriskiin varautumisen keinona ja sen hyödyllisyydestä ei olla vakuuttuneita.

Seuraavassa taulukossa on koottu yhteenvetona yrityksien ja vakuutusyhtiöiden edustajien mielipiteitä riskin havaitsemisesta, siitä miten hyvin yritys pystyy suoriutumaan riskin sattuessa sekä kuinka hyödyllisinä kybervakuutuksen palveluita pidetään. Lisäksi on listattu, miten kybervakuutuksen hinta koetaan sekä millaisena kybervakuutuksen tulevaisuus nähdään.

	Yrityksien mielipiteet	Vakuutusyhtiöiden mielipiteet
Riskin havaitseminen	Riskiä pidetään suurena	Riskiä pidetään suurena
Riskin sattuessa	Yritys pystyy suoriutumaan itse	Yritys ei välttämättä pysty suoriutumaan itse
Kybervakuutuksen palveluiden hyödyt	Eivät koe niin hyödyllisinä	Kokevat erittäin hyödyllisinä
Kybervakuutuksen hinta	Pidetään kalliina	Pidetään halpana
Kybervakuutuksen menestys	Eivät näe tuotteella välttämättä tulevaisuutta	Tuotteen tulevaisuus koetaan hyväksi

Kuvio 6. Yrityksien ja vakuutusyhtiöiden edustajien mielipiteet kyberriskistä sekä kybervakuutuksesta.

Taulukosta voidaan nähdä, että ainut asia, missä yritykset ja vakuutusyhtiöt olivat samaa mieltä, oli se, että riski koetan suurena. Tästä voidaan muodostaa johtopäätelmä siitä, että vaikka he pitävät molemmat riskiä yhtä suurena, he katsovat sitä eri näkökulmista sekä suhtautuvat siihen eri tavalla. Yritykset ovat hyvin optimistia sen suhteen, miten heidän yritys pystyisi riskin toteutuessa toimimaan, kun taas vakuutusyhtiöt ovat skeptisempiä. Sitä, kumman näkemys on realistisin, on hyvin vaikea sanoa. Vakuutusyhtiöt ovat riskienhallinnan ammattilaisia, mutta toisaalta taas yrityksillä on tuntemus omasti liiketoiminnastaan ja sen vahvuuksista ja heikkouksista. Se, liikkuvatko yrityksien ja vakuutusyhtiöiden mielipiteet lähemmäksi vai kauemmaksi toisiaan tulevaisuudessa on mielenkiintoista nähdä. Ainoastaan tulevaisuuden toteutuneet kyberriskit, jotka tuovat kokemusta kybervakuutuksesta ja sen ominaisuuksien tarpeellisuudesta riskin sattuessa, tulee näyttämään pääsevätkö yritykset ja vakuutusyhtiöt mielipiteissään lähemmäksi toisiaan. Se, että mielipiteet vakuutettavalla ja vakuuttajalla eroavat noinkin paljon toisistaan, vaikuttaa selkeästi kybervakuutuksen myyntiin negatiivisesti. Vakuutusyhtiöiden olisikin tärkeää saada kuilu mielipiteiden välillä pienemmäksi, jotta kybervakuutuksen myyntivolyymia saataisiin nostettua.

Vakuutusyhtiöiden edustajien mukaan yritykset helposti ajattelevat, että tämä riski ei koske meitä. Usein ajatellaan, että Suomi on tavallaan eristyksissä tai yritys on kooltaan niin pieni, ettei kukaan sitä hakkeroisi. Tämän tutkimuksen valossa yritykset tiedostavat riskin hyvin ja mieltävät olevansa riskillä, mutta ovat hyvin optimistia siitä, miten pystyvät vastaamaan riskiin oman organisaation voimin. Aikaisempien tutkimuksien mukaan taas alle puolet tutkituista IT-ammattilaisista ja IT-tarkastajista olivat sitä mieltä, että heidän yrityksensä voisi havaita sekä vastata vakavaan tietomurtoon. Molemmat haastateltavat yritykset olivat sitä mieltä, että heidän oman IT-osaston resurssit riittäisivät kyberrikoksen selvittämiseen ja siitä johtuvien seurauksien kattamiseen. Vakuutusyhtiön edustajien mukaan yritykset saattavat tässä kohtaa olla turhan itsevarmoja, koska kyberhyökkäys on ainutlaatuinen eikä liity IT-osaston päivittäiseen työhön. Suurin näkemysero yritysten sekä vakuutusyhtiöiden asiantuntijoiden välillä oli juuri se, miten yhtiöt pystyisivät itse vastaamaan kyberhyökkäykseen. Yritykset ovat itse optimistisia, kun taas vakuutusyhtiöt skeptisiä asian suhteen. Se, millaiset resurssit yrityksillä on vastata kyberhyökkäykseen, riippuu täysin yrityksestä sekä sen IT-osastosta tai palveluntarjoajasta. Vain sattuneen hyökkäyksen jälkeen saa nähdä oliko kontrollit todella niin paikallaan, kuin niiden olisi pitänyt olla, tai onko oma IT-osasto tai ulkoinen palveluntarjoaja tarpeeksi osaava.

Tämä tutkimuksen aikana esiin tullut asia vakuutusyhtiöiden ja yrityksien mielipiteiden eroavaisuuksista on erittäin mielenkiintoinen ja se, ovatko yritykset liian itsevarmoja vai ovatko

vakuutusyhtiöt liian skeptisiä asian suhteen, on mahdotonta tämän tutkimusasetelman valossa sanoa.

Molemmat suomalaiset yritykset, joita haastattelin, olivat kärsineet niin syntaktisista sekä semanttisista kyberhyökkäyksistä. Yritys B, joka ei käytä ulkoisia palvelutarjoajia oli suoriutunut hyökkäyksistä oman IT-osaston avulla ainakin tähän päivään saakka. Vaikea sanoa, olisiko asia eri tavalla erilaisten kohdennettujen hyökkäyksien osalta tai miten asia tulee muuttumaan tulevaisuudessa riskien muuttaessa muotoaan. Vaikea on arvioida myös sitä, olisiko yritykset suoriutuneet nopeammin ja pienimmillä haitoilla, jos heillä olisi ollut kybervakuutus ja sen mukana tulevat palvelut. Toisaalta silloin yrityksillä olisi ollut nykytilanteeseen verrattuna huomattava lisäkulu kybervakuutusmaksuista.

Kybervakuutuksen mukana tulevien palveluiden hyödyt koettiin erilaisiksi yrityksien ja vakuutusyhtiöiden välillä. Yritykset eivät kokeneet palveluita tarpeellisena, kun taas vakuutusyhtiöiden mielestä ne ovat hyvin relevantteja, jotta kybertapahtuma saadaan paikannettua ja käsiteltyä. Kybervakuutuksen mukana tulevia palveluja voidaan pitää pienten yritysten kannalta merkittävimpinä kuin suurten yritysten, koska pienillä ei ole välttämättä omaa IT-osastoa eikä muutenkaan niin suurta osaamista ja tietämystä kuin suurilla yrityksillä. Pienet yhtiöt myös saavat kybervakuutuksen mukana tulevat palvelut halvemmalla, kuin tilanteessa jossa ostaisivat ne itse. Vakuutusyhtiöiden IT-kumppanien voidaan nähdä myös suurten yritysten kohdalla heikentävän myyntiä, koska yritykset haluavat usein käyttää omia palveluntarjoajiaan. Tästä muodostuu kuitenkin myös ristiriita, koska usein kybervakuutus on suunniteltu suuryritysasiakkaille, joilla on maksukykyä, mutta tämän tutkimuksen valossa näyttäisi siltä, että pienet yritykset hyötyvät tuotteesta paremmin ainakin IT-palveluiden osalta. Kybervakuutukselle siis tunnusomaista on vakuutusyhtiöiden yhteistyö IT-konsultointi yrityksen kanssa, mikä erottaa sen muista perinteisistä vakuutustuotteista. Kumppaneiden käytöllä on kuitenkin myös haittapuolensa, mutta kaikkea ei vakuutusyhtiön kannata tai ole edes mahdollista tehdä itse.

Aikaisempien tutkimuksien mukaan on monia kustannuksia joihin yritykset eivät ole osanneet varautua ja näitä ovat muun muassa oikeudenkäyntikulut, maineen menetys ja kybervakuutusmaksujen nousu. Vakuutusyhtiöiden edustajat ovat samaa mieltä, että yritykset eivät ole välttämättä täysin ymmärtäneet, miten laajaa-alaisia ja kauaskantoisia kustannuksia kybertapahtumat voivat aiheuttaa. Tämän tutkimuksen perusteella kyberriskien laajuus on kyllä ymmärretty, mutta kaikkia mahdollisia seurauksia ei välttämättä ole tiedostettu. Kybertapahtumat eivät kos-

keta vain yhtä osastoa yhtiöstä vaan voivat vaikuttaa koko organisaatioon, jolloin riski on moniulotteinen. Molemmilla yrityksillä hyökkäykset ovat olleet sitä kokoluokkaa, ettei suuria kustannuksia tai haittaa yhtiölle ole ehtinyt tapahtumaan.

Tutkimuksien mukaan yritysten pitäisi tehdä kyberriski stimulaatioita, jotta riskin toteutuessa organisaatiolla olisi valmiudet ja tieto siitä, kuinka toimia. Organisaatiossa A tehdäänkin simulaatioita, joissa testataan tietosuojajärjestelmien toimivuutta. Kyberriskit ovat myös integroitu osaksi strategista suunnittelua. Organisaatio B on taas huomattavasti pienempi kuin A ja heillä ei simulaatioita ole vielä toistaiseksi ainakaan tehty. Kyber ilmiönä vaatii yrityksiltä rahaa ja se on selkeästi suurten yritysten ”riskitrendinä”. Yritykset varautuvatkin kyberriskeihin omien budjettiensa rajoissa. Varautumiseen vaikuttaa myös se, kuinka relevanttina riskiä pidetään omalle organisaatiolle.

Suomen kybervakuutusmarkkinat ovat hyvin pienet verrattuna muihin maihin. Kybervakuutuksen osuus vakuutusyhtiöiden tuotteista on vain muutaman prosentin luokkaa ja kilpailu markkinoilla on pääosin ulkomaalaisten yhtiöiden hallinnassa. Suomen markkinoilla kybervakuutusten hinnat ovat todella alhaalla verrattuna muihin maihin, koska dataa ei ole ja vahinkokehitys on vielä niin pientä. Vahinkojen lisääntyessä hinnat tulevat myös nousemaan, joten otollinen aika tuotteen hankinnalle olisi nyt. Kybervakuutusmarkkinoille on tulossa vuonna 2017 myös lisää suomalaisia toimijoita, kun LähiTapiola lanseeraa oman tuotteensa. Kybervakuutusmarkkinat ovat kasvaneet jatkuvasti ja jatkavat kasvuaan, mikä kiristää kilpailua. Tutkimuksesta käy ilmi, että Suomen kybervakuutusmarkkinoilla kilpailevat vakuutusyhtiöt koittavat asemoitua markkinoilla ja tarjota sellaista lisäarvoa asiakkaille mitä kilpailija ei tarjoa. Tuotteen pienestä vakuutusmaksutulosta sekä pienestä prosentuaalisesti osuudesta verrattuna muihin vakuutustuotteisiin huolimatta kilpailu on kovaa.

Tuotteen myyntiprosessit ovat suuryritysasiakkaille vielä pitkiä ja työläitä, koska yrityksen tietoturvataso on tarkastettava erilaisten tietoturvaselvitysten avulla. If:n pienille ja keskisuurille yritysasiakkaille kybervakuutuksen myynti onnistuu 2017 vuoden puolella netissä, mikä osaltaan helpottaa ja nopeuttaa myyntiprosessia. Vakuutusyhtiöiden edustajien mukaan ennakoivaohjaus lisää nimenomaan tietoisuutta uhkista sekä itse vakuutustuotteesta ja toimii näin myynninedistämisenä. Yhtiöt myös käyttävät ennakoivaa ohjausta yhtenä kilpailutekijänä. Kybervakuutuksen myynti koetaan hankalaksi, koska riski koskee niin montaa eri organisaation osastoa, jolloin päätöksentekoprosessiin sisältyy useampi henkilö. Yhtiöiden IT-osastot ovat

osoittautuneet suurimmiksi kybervakuutuksen oston vastustajiksi. Riskienhallinnan osaston tulisi arvioida kulut mitä aiheutuu, jos riski pidetään itsellä eikä vain suoraan ajatella kybervakuutusta menoeränä vaan punnita mitä menoja aiheutuu, jos riskiä ei siirretä. Myyntiprosessin monimutkaisuus on varmasti osaltaan myös yksi tekijä kybervakuutuksen hitaaseen omaksumiseen Suomessa. Koska kyberriskejä ei voi konkreettisesti havaita eikä niillä ole maantieteellisiä rajoja, saatetaan ilmiö kokea mystisenä. Tuotteen yksinkertaistaminen ja mystiikan poistaminen onkin toiminut kilpailullisena tekijänä If:lle.

Oman organisaation juristeilla ja IT-osastolla ei ole välttämättä juuri kyberriskeihin liittyvää osaamista. Juristit hallitsevat todennäköisesti sopimusoikeuden, mutta eivät välttämättä tiedä miten toimia tilanteessa, jossa asiakastiedot ovat vuotaneet ulkopuolisille. IT-osasto taas on tottunut tekemään organisaation sisäisiä järjestelmiä sekä niiden ylläpitoa ja pystyy suoriutumaan varmasti pienimmistä kyberriskeistä. Kun kysymykseen tulee kohdennetut hyökkäykset tai kiristysohjelma, on niihin tottunut IT-konsultti nopeampi ja parempi apu. Tässä kohtaan esiin nousee taas se, että kyberriskit ovat uusia riskejä ja poikkeavat organisaatioiden eri osastojen ammattilaisten normaaleista haasteista.

Vakuutusyhtiöille kybervakuutus on tietenkin kasvumahdollisuus, koska kyberriskit ovat lisääntyneet ja lisääntyvät jatkuvasti. Siksi yhä useampi vakuutusyhtiö pyrkii markkinoille. AIG oli ensimmäinen, joka toi kybervakuutuksen markkinoille niin Suomessa kuin muualla maailmassa. Kybervakuutuksien kehityksessä on siirrytty tuotteiden sekä asiakkaiden segmentointiin. Tämä on nähtävissä myös Suomessa, koska osa targetoi vain suuria yrityksiä ja osa vain pieniä. Verrattuna Yhdysvaltojen markkinoihin Suomessa vakuutustuotteen segmentointi ei ole vielä niin pitkällä. Yhdysvalloissa on edetty pitkälle asiakkaiden segmentointiin ja kapeat korvauspiirit houkuttelevat erilaisia asiakkaita. Tulevaisuudessa kilpailun lisääntyessä tuotteita tullaan varmasti segmentoimaan lisää ja tuotteesta tulee olemaan esimerkiksi erilaisia turvatasoja. Tämä tulee varmasti kiihdyttämään kybervakuutusmarkkinoiden kasvua, kun kybervakuutus pystyy palvelemaan yhä erilaisempia organisaatioita. Kyberriskien monimuotoisuudesta johtuen yksi kybervakuutustuote ei mitenkään pysty palvelemaan kaikkia yrityksiä ja siksi tarvitaankin segmentointia.

Jälleenvakuutus on erittäin tärkeässä roolissa tällaisessa riskissä, jonka kokoluokkaa ei voi etukäteen arvioida. Systeemiriski ja riskin keräytyminen on huolestuttava, koska kyberriskeillä ei ole fyysisiä rajoja jonka vuoksi ne haastavatkin mallinnusskenaariot. Jälleenvakuutusta tarvitaan, jotta isojen yritysten tarpeisiin riittävän suuria vakuutusmääriä pystytään myymään. Riski

on kumuloituva, joten vakuutuskannan sekä jälleenvakuutuksen on oltava todella suuria, jotta riskiä voidaan kantaa. Kybertapahtumat voivat nykyään aiheuttaa myös fyysistä vahinkoa. Vakuutusyhtiöt ovatkin koittaneet luoda uusia tuotepaketteja, jotka kattaisivat molemmat riskit. Kuitenkaan uutena riskinä tätä ei voida pitää, koska fyysistä vahinko aiheuttavia riskejä on ollut aina ennen kybervahinkoja, joten periaatteessa tämä on katsomista vain taaksepäin.

Molemmat yritykset näkivät kybervakuutuksen oston ainakin vielä toistaiseksi kaukaisena ideana ja hieman epätodennäköisenäkin. Tämä vahvistaa osittain myös aikaisempaa teoriaa, jonka mukaan kybervakuutustuotteen kanssa on ollut ongelmia niin vakuutuksenottajilla kuin -antajilla. Kyberriskit ovat korreloituneita ja yhtiöillä on vaikeuksia todistaa tietomurrosta aiheutuneet haitat. Kybervakuutuksen hitaaseen omaksumiseen vaikuttaa myös puutteellinen informaatio sekä uskominen, että kyberriskien ehkäisyyn panostaminen on parempi kuin vakuutuksen osto. Tämän tutkimuksen perusteella voidaan sanoa, että tiettyyn pisteeseen asti kyberriskien ehkäisyyn panostaminen onkin parempi ja välttämätön valinta kuin vakuutuksen osto. Tietoturvan on oltava myös ylipäätään kunnossa, jos kybervakuutusta mielii ostaa.

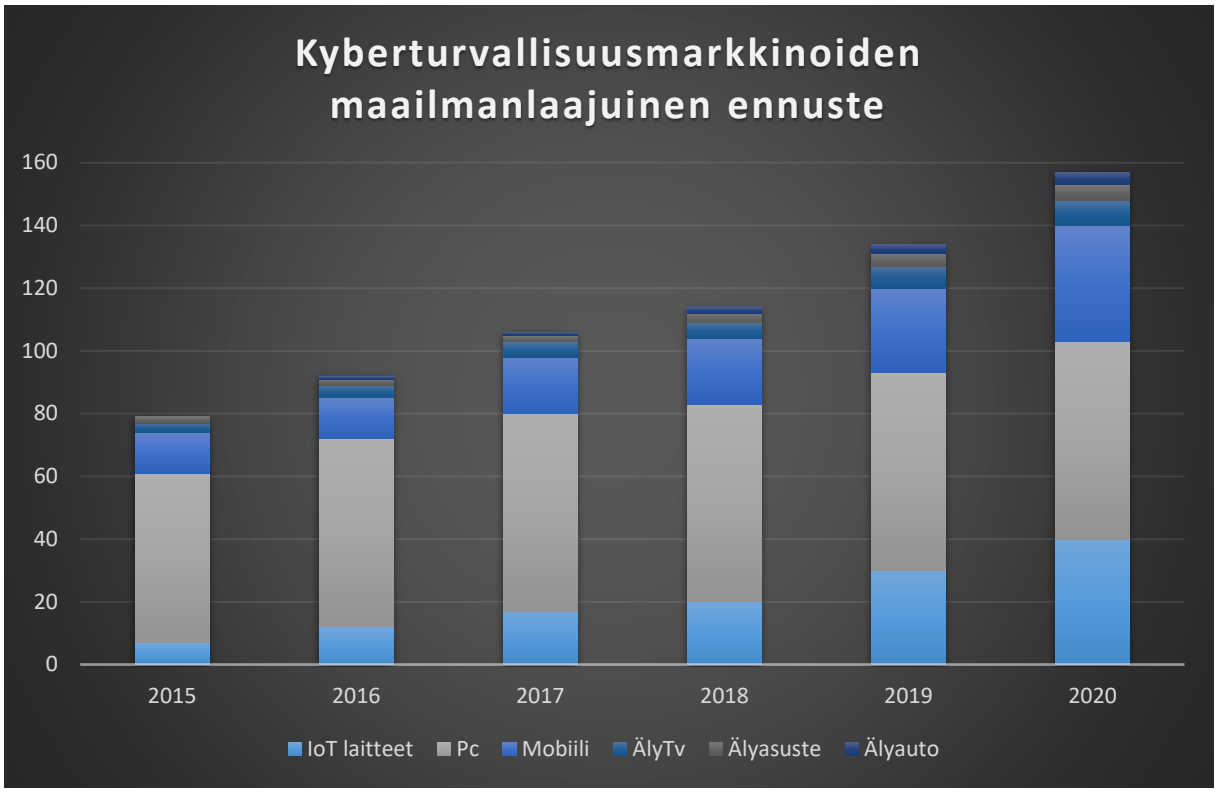
Haitalliseen valikoitumiseen vastatakseen vakuutusyhtiöiden täytyy suorittaa yrityksen läpi yksityiskohtainen riskiarviointi. Ehtona vakuutuksen saamiselle on riskiarvioinnin tekeminen, jossa vakuutusyhtiö arvioi ja käy läpi lukemattomia yrityksen prosesseja saadakseen selvyyden yrityksen haavoittuvuudesta. Yhtiöt eivät yleensä halua kuitenkaan paljastaa tietosuojansa tasoja, jotta tieto ei leviä ulkopuolisille sekä mahdollisesti hakkereiden käsiin. Tämä onkin osaltaan vaikeuttanut kybervakuutuksen myyntiä, koska vakuutusyhtiön on saatava tietyt tiedot yritykseltä, jotta ovat valmiita myöntämään vakuutuksen, mutta jotkut yritykset ovat kokeneet, että joutuvat paljastamaan liikaa tietoja. Kybervakuutuksen myynnissä on tärkeää löytää avainkysymykset yrityksen haavoittuvuudesta, jotta riskiä voidaan mitata oikein. Kybervakuutustuotteen kohdalla ei siis olla paljoa törmätty haitalliseen valikoitumiseen ja moraalikatoon, koska tuote on hintava ja sen myyntiprosessi on pitkä. Nämä seikat mitkä vähentävät haitallista valikoitumista ja moraalikatoa taas osaltaan voivat pienentää ostajakuntaa, koska yritykset eivät halua paljastaa arkaluonteista informaatiota mitä tarvitaan kyberriskianalyysin tekemiseen myyntivaiheessa.

Se ottaako yritys kybervakuutusta vai ei riippuu siitä, miten he arvioivat riskin omalla kohdallaan. Riskin havaitseminen voi yrityksillä perustua myös virheellisiin analyyseihin. Lähtökohtaisesti kaikki, joilla on asiakastietoja joillakin palvelimilla altistuvat tälle riskille. Vaikka yritykset tietäisivätkin riskistä, monet saattavat sulkea silmänsä siltä. Kyberriski nähdään joissakin

yrityksissä edelleen riskinä, josta ajatellaan, että eihän se meille satu. Voi olla, että yritykset ajattelevat kyberriskin vielä niin kaukaiseksi ja jopa hieman vaikeaksi käsittää, mikä osaltaan vaikuttaa siihen, että siltä suljetaan silmät tai sitä vähätellään, koska se on laajuudeltaan niin suuri eikä fyysisesti läsnä. Tosin vaikka yritykset olisivat hyvinkin tietoisia riskistä, niin kuin tässä tutkimuksessa, eivät he siltikään koe välttämättä kybervakuutusta tarpeelliseksi kyberriskienhallintakeinoksi.

Mitä enemmän vahinkoja sattuu, sitä konkreettisemmaksi riski tulee. Kyberriskit ovat kuitenkin nykypäivää. Julkisuuteen ei myöskään kantaudu läheskään kaikki esimerkiksi Suomessa sattuneet kyberhyökkäykset, mikä taas osaltaan vääristää todellisuutta. Vielä harvemmin julkisuuteen päätyy kyberhyökkäyksistä vaadittuja vakuutuskorvaussummia, mikä taas luo vaikutelman, että ennakkotapauksia ei ole niin paljoa, joten helposti ajatellaan, että eihän tässä millään suurella riskillä olla. Verrattuna esimerkiksi Yhdysvaltoihin ja Iso-Britanniaan Suomessa kyberriskeistä uutisoiminen on vielä vähäistä. Tämä johtuu osaltaan siitä, että hyökkäyksiä on sattunut tietenkin suhteessa vähemmän, mutta myös siitä, että tutkimusta ei ole tehty niin paljoa eikä jo sattuneista hyökkäyksistä puhuta. Vaikka Suomi on pieni maa ja maantieteellisesti niin sanotusti eristyksissä, on riski silti yhtä suuri, koska kyberriskillä ei ole maantieteellisiä rajoja.

Maailman kybervakuutusmarkkinoista 90 prosenttia hallitsee Yhdysvallat. Suomen kybervakuutusmarkkinat ovat siis vielä pienet ja vakuutusehdot sekä korvauskäytännöt hakevat omia uomiaan. Kyberturvallisuus on kasvava markkina ja tulevaisuudessa kyberilmiö tulee olemaan vielä enemmän esillä. Kyberturvallisuusmarkkinoiden maailmanlaajuisesta kasvusta on erilaisia ennusteita, mutta kaikkia niitä yhdistää se, että markkinoiden kasvun ennustetaan olevan nopea.



Kuvio 7. Kyberturvallisuusmarkkinoiden maailmanlaajuinen vuotuinen kasvuennuste. (www.businesinsider.com 2016)

Yllä olevassa taulukossa on kuvattu kyberturvallisuusmarkkinoiden vuotuista kasvua maailmanlaajuisesti. Taulukossa olevat summat ovat Yhdysvaltain biljoonissa dollareissa. Vuoteen 2020 mennessä kyberturvallisuusmarkkinoiden oletetaan kasvavan lähes 160 biljoonaan dollariin vuoden 2016 reilusta 90 biljoonasta dollarista. Kasvu muodostuu tietoverkkoon liitettyjen laitteiden kasvuosuuksista. Suurimman osan kasvusta selittää IoT eli ”internet of things” laitteiden kasvu. Lisäksi mobiililaitteiden lisääntyvät tietoturvauhkat kasvattavat markkinoita myös huomattavasti. Pc-koneiden osuus markkinoista pysyy melko samana tulevina vuosina ja näin ollen markkinoita kasvattavatkin uudet tietoverkkoon yhdistetyt keksinnöt. Älyasusteet ”wearables” kasvattavat markkinoita voimakkaammin kuin aikaisemmin vuoden 2017 jälkeen samoin kuin älyautot. Älyautot kattavat pienimmän osan markkinoista vielä toistaiseksi, mutta kasvua on selkeästi nähtävissä ennusteen mukaan.

Kuten voi huomata kybermarkkinoista tavalliset pc-laitteet vievät vielä suurimman osan, mutta kasvua ne eivät enää selitä. Teknologia ja sen murros lisäävät tietoverkkoon yhdistettyjen laitteiden määrää ja mitä useampia uusia teknologia keksintöjä muodostuu, sitä suuremmiksi myös

kyberturvallisuusmarkkinat kasvavat. Näin ollen voisi päätellä, että maailmanlaajuiset kyberturvallisuusmarkkinat jatkavat nopeaa kasvamista pitkällä tulevaisuudessakin. Tämä ennuste näyttää lupaavalta myös kybervakuutuksen näkökulmasta, koska markkinoiden kasvaessa myös riskit lisääntyvät, jolloin tietoisuus niistä myös kasvaa samoin niiden vakuuttamisen tarve.

Kaikesta huolimatta kybervakuutus ei ole toistaiseksi vielä lähtenyt kunnon nousukiitoon Suomen vakuutusmarkkinoilla. Syitä tähän voidaan tämän tutkimuksen perusteella löytää useita. Tuote nähdään hankalana sekä epäselkeänä ja sen vakuutuskorvauksen hyödyllisyydestä ollaan skeptisiä eikä ihme, sillä kybervakuutuksessa on monta moduulia ja riskikokonaisuutta, joita voidaan vakuuttaa. Samankokoinen tuote ei voi millään palvella kaikkia yrityksiä, siksipä segmentointi tuotteen osalta on tulevaisuudessa entistä tärkeämpää niin kybervakuutuksen myynnin kuin riskiltä suojautumisenkin kannalta. Riski näyttäytyy erilaisena eri toimialoille ja markkinat tulevat kasvamaan, kunhan tuotetta segmentoidaan lisää. Vakuutuksien korvauspiirejä voi olla myös vaikea käsittää, eikä varsinkaan pienissä yrityksissä toimitusjohtajalla ole välttämättä hyvää käsitystä siitä, mitä on jo vakuutettu ja mitä pitäisi vielä vakuuttaa. Lisää haasteita tuo juuri se, että kyber vaikuttaa organisaation moniin eri osastoihin, jolloin voi muodostua haasteeksi se, mistä budjetista kybervakuutus ostetaan. Tämän tutkimuksen tulosten perusteella yksi iso tekijä on juuri yritysten sekä vakuutusyhtiöiden näkemyserot tuotteesta ja sen tarpeellisuudesta. Kuilu näiden näkemyserojen, jotka on esitetty kuviossa 6. välillä pitäisi saada pienemmäksi, jotta kybervakuutus tulisi Suomessa menestymään paremmin.

Kybervakuutus ei kuitenkaan ole kaikkia varten, kuten muut vielä nykypäivänä yleisemmät vakuutukset. Jotkin yritykset voivat pärjätä nyt ja myös tulevaisuudessa ilman sitä, jos he pystyvät kyberrikoksen sattuessa jatkamaan liiketoimintaansa muulla tavoin. Riski maineen menettämisestä on kuitenkin siitä huolimattakin olemassa, vaikka yritys pystyisikin jatkamaan liiketoimintaansa. Koska riskienhallinnassa on monia muitakin vaihtoehtoja kuin vakuutus, ei se oli kaikille se välttämätön ratkaisu. Tarpeettomasta turvasta ei kukaan halua maksaa.

Kaikesta huolimatta voidaan silti todeta, että Suomessa kybervakuutuksella on kuitenkin hyvät lähtökohdat menestyä, kun katsoo ennusteita kyberturvallisuusmarkkinoista sekä miten kybervakuutusmaksutulot ovat maailmanlaajuisesti kasvaneet vuosi vuodelta. Tärkeää on vain saada yritykset ja vakuutusyhtiöt samalle viivalle kybervakuutuksen tarpeellisuudesta. Kybervakuutus on molemmin puolin koettava samanlaisena ja sen ominaisuuksien on oltava sellaisia, joista yritykset ovat valmiita maksamaan. Vaikka yritysten riskitietoisuus on jo hyvällä tasolla, uusien

sattuneiden vahinkojen myötä riski konkretisoituu vielä enemmän ja kybervakuutuksen segmentointi Suomen markkinoilla tulevaisuudessa varmasti pienentää yrityksien ja vakuutusyhtiöiden näkemyserojen kuilua, kun tuote muokkautuu enemmän erilaisten yritysten tarpeiden mukaisesti. Yhteenvetona voidaan myös todeta, että kybervakuutus tuotteena käsittää monia eri osa-alueita ja riskiarviointityö on niin vakuutusyhtiöiden kuin vakuutuksenottajienkin asemassa hankalaa. Uudenlaisia riskejä syntyy ja kyberriski on esimerkki riskistä, jonka laajuutta on hyvin vaikea käsittää. Tietotekniikka vaikuttaa kuitenkin nykypäivänä suurimman osan yhtiöistä kaikkiin liiketoiminnan prosesseihin. Näin riskin voidaan nähdä kulkevan läpi koko organisaation, jolloin riski on massiivinen.

6.2 Tutkimuksen arviointi ja jatkotutkimusehdotukset

Kaikissa tutkimuksissa pyritään arvioimaan tutkimuksen luotettavuutta. Tutkimuksen luotettavuuden arvioinnissa puhutaan reliabiliteetista sekä validiteetista. Reliaabelius tarkoittaa tutkimuksen toistettavuutta, eli se mittaa tutkimuksen kykyä antaa ei-sattumanvaraisia tuloksia. Reliaabeliutta voidaan testata esimerkiksi sillä, jos kaksi arvioijaa päätyy samaan tulokseen. Validius taas liittyy tutkimusmenetelmän kykyyn mitata juuri sitä, mitä on tarkoituskin mitata. Validius merkitsee myös tutkimuksen kuvauksien ja siihen liitettyjen selitysten yhdenmukaisuutta. Validointitapana voidaan pitää myös lähteiden luotettavuutta, eli edustaako haastateltavat sitä ryhmää, joiden heidän oletetaan edustavan. (Hirsijärvi & Hurme 2011, 188)

Mahdollisimman nopeasti haastattelun jälkeen tapahtuva litterointi parantaa tutkimuksen laatua. Haastatteluaineiston luotettavuuden takaamisessa on tärkeää, että kaikki haastattelut litteroidaan yhtä tarkasti ja samalla tavalla. Aineiston olosuhteet olisi myös kerrottava mahdollisimman selvästi esimerkiksi ajat ja paikat, missä aineistot kerättiin. Lisäksi on tärkeää, että tutkija kertoo oman itsearvioinnin tilanteesta ja sen kulusta. Tutkijan on myös pystyttävä perustelemaan millä perusteella hän esittää tulkintoja aineistosta. Tässä on etua siitä, jos tutkimukseen lisätään suoria haastatteluotteita tutkimusaineistosta. (Hirsijärvi ym. 2009, 232) Tämän tutkimuksen luotettavuutta on pyritty lisäämään haastatteluprosessin tarkalla kuvauksella ja tutkimuksesta johdettujen johtopäätelmien selkeällä dokumentoinnilla tutkimusraportissa. Lisäksi tutkimuksessa on käytetty suoria lainauksia haastatteluiden relevanteista otteista, jolloin päätelmien perusteluille saadaan vielä enemmän luotettavuutta. Teemahaastattelut toimivat

tässä tutkimuksessa hyvin ja niiden avulla saatiin syvällistä tietoa sekä uusia näkökulmia ja ulottuvuuksia tutkimukseen.

Tutkimuksen yleistettävyydessä on kuitenkin syytä huomioida, että jos haastateltavilla yrityksillä olisi sattunut olemaan kybervakuutus olisivat tutkimustulokset olleet osittain erilaisia. Myöskin, jos yritykset olisivat työskennelleet toimialalla, jossa altistutaan vähemmän kyberriskeille, olisi se myös vaikuttanut tutkimustuloksiin. Tutkimuksessa haluttiin kuitenkin nimenomaan valita sellaiset yritykset, jotka altistuvat paljon kyberriskeille ja näillä yrityksillä ei siitä huolimatta ollut kybervakuutusta. Nämä yritykset eivät kuitenkaan kuulu liikevaihdoltaan Suomen top isoimpiin yrityksiin ja tutkimuksen teon aikana kävi ilmi, että Suomessa ne yritykset joilla kybervakuutus on ovat suurilta osin kansainvälisiä konserneja.

Tutkimusta tehdessä on mietitty myös jatkotutkimusehdotuksia. Tässä tutkimuksessa on keskitytty tutkimaan sitä, miten suomalaiset yritykset ovat varautuneet ja tiedostaneet kyberriskit sekä tarkastelemaan Suomen kybervakuutusmarkkinoiden tilaa vuonna 2016. Tässä on tarkasteltu kybervakuutusta uutena tuotteena ja pyritty saamaan käsitys kybervakuutustuotteesta vakuutuksenantaja sekä -ottajan näkökulmasta. Koska aihe on Suomessa vielä vähän tutkittu, jatkotutkimusehdotuksia löytyy aiheesta useita. Koko tutkimuksen voisi tehdä esimerkiksi keskittyen kybervakuutukseen vakuutuksenantajan näkökulmasta, jolloin tuotetta ja sen ominaisuuksia voisi tutkia vielä paljon syvällisemmin. Tutkimuksessa voisi keskittyä näin ollen esimerkiksi kybervakuutuksen juridiseen tai tekniseen puoleen. Tutkia voisi myös pelkästään kyberriskejä esimerkiksi yhteiskunnallisesta näkökulmasta katsottuna, jolloin tutkimuksen kohteeksi voisi ottaa Suomen kyberturvallisuusstrategian. Kyberriskit yhteiskunnan näkökulmasta eroavat paljonkin yrityksen näkökulmasta, jolloin tutkimukseen muodostuu täysin eri näkökulmia. Kyberilmiö on ollut mediassa trendinomaisesti nyt muutaman vuoden ajan ja sitä voi lähteä tutkimaan useista eri näkökulmista.

LÄHDELUETTELO

Kirjallisuus:

Bandyopadhyay Tridib, Mookerjee Vijay S, Ram C. Rao. 2009. Why IT Managers Don't Go for Cyber-Insurance Products? Communications of the ACM, Vol. 52 No. 11, p. 68-73

Bendovschi. 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, Vol. 28, 24-31

Biener Christian, Eling Martin and Wirfs Jan Hendrik. 2015. Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance, 40, p.131–158

Choo, Kim & Kwang Raymond. 2011. The cyber threat landscape: Challenges and future research directions. Computers & Security. Vol 30 Issue 8

Gregg Robert. 2010. The CFO's Role in Managing Cyber Risk. Financial Executive, 26, 7, p. 61-62, Financial Executives International

Hardy, Karen, Runnels & Allen. 2015. Enterprise Risk Management: A Guide for Government Professionals. San Francisco, California: Jossey-Bass, 2015

Hathaway Oona, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William and Spiegel Julia. 2012. The Law of Cyber-Attack. California Law Review, Vol. 100, No. 4. p. 817-885

Hirsijärvi, Remes & Sajavaara. 2009. Tutki ja kirjoita. Helsinki: Tammi

Hirsijärvi & Hurme. 2008. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press

Hulisi Ogut, Srinivasan Raghunathan & Nirup Menon. 2011. Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. Risk Analysis and International Journal, Vol. 31, No. 3

Ilmonen, Kallio, Koskinen & Rajamäki. 2013. Johda riskejä. Finanssi- ja vakuutuskustannus Finva: Helsinki

Jones Robert. 2015. Cyber Insurance: What You Should Know? Insurance Advocate, 126, 20, p. 28-30, CINN Worldwide Inc

Keegan C. 2014. Special Issue on Security in the Cyber Supply Chain.Volume 34, Issue 7, p. 380–381

Limnell, Jarno. 2014. Kyber rantautui Suomeen. Aalto-yliopiston julkaisusarja

Lawrence A., Gordon Martin P, Loeb, and Tashfeen Sohail. 2003. Communications of the ACM. Vol. 46, No. 3

Majuca, Yurcik & Kesan. 2005. The evolution of cyber insurance. Department of Economics; National Center for Supercomputing Applications (NCSA) College of Law

McCollum Tim. 2015. The cybersecurity Imperative. (cover story) Internal Auditor, Vol.72, Issue. 4, p. 26-31.

Mossburg, Emily. 2015. A Deeper Look AT THE Financial Impact OF Cyber Attacks. Financial Executive, Vol 31, 3, p.77-80, Financial Executives International

Mukhopadhyay Arunabha, Saha Debashis, Chakrabarti, Mahanti Ambuj & Podder Asok. 2005. Decision, Vol. 32, No.1, January - June, 2005

Nierengarten Nick. 2006. A Plan for Wealth Managers to Reduce the Risk of Cyber Threats. Journal of Wealth Management. Winter 2006, Vol. 9 Issue 3, p. 24-30.

Quigley Kevin, Burns Calvin, Stallard Kristen. 2015. 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. Government Information Quarterly, Vol. 32, 2, p.108–117

Rantala & Kivisaari. 2014. Vakuutusoppi. Finanssi- ja vakuutuskustannus Finva: Helsinki

Shackelford, Scott J. 2012. Should your firm invest in cyber risk insurance? Bus.Horiz. Vol. 55, 4, p. 349-356

Skopik Florian, Settanni Giuseppe & Fiedler Roman. 2016. A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Computers & Security. Accepted manuscript.

Smith Kate. 2016. Cyber Sabotage. Best's Review, 10, p. 42-45, AM Best Company Inc

Tuomi Jouni & Sarajärvi Anneli. 2009. Laadullinen tutkimus ja sisällön analyysi. Tammi: Helsinki

Yang Zichao, Lui John. 2014. C.S.Security adoption and influence of cyber-insurance markets in heterogeneous networks. Performance Evaluation, 74, 1-17

Voelker Michael. 2015. Cyber: Ready for Takeoff. Property & Casualty 360, 119, 13, p. 42-49, ALM Media, LLC

Zelle Anthony, Whitehead Suzanne M. 2014. Cyber Liability: It's Just a Click Away. Journal of Insurance Regulation. Vol. 33, p. 145-168.

Internet-lähteet:

Allianz Global Corporate & Specialty: A Guide to Cyber risk 2015 (18.4.2016)

http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

Application Vulnerability Trends Report. 2014 (10.4.2016)

https://www.info-point-security.com/sites/default/files/cenzic-vulnerability-report-2014.pdf

Business insider 2016. (20.2.2017)

http://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3?r=US&IR=T&IR=T

COSO 2004. Enterprise Risk Management - Integrated Framework. (10.4.2016)

http://www.coso.org/documents/coso_erm_executivesummary.pdf

European Union Agency for Network and Information Security 2015 (15.3.2016)

https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/enisa-threat-landscape-top-15-cyber-threats-2015

International Organization for Standardization (ISO) 2010. A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000 (10.4.2016)

http://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf

International Risk Management Institute, Inc. Cyber insurance market survey. Betterley. 2015 (10.3.2016)

https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf

PwC: Information Security Breaches Survey 2015 (2.3.2016)

http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

Risk Management Handbook. University of Adelaide. (2.3.2016)

http://www.adelaide.edu.au/legalandrisk/docs/resources/Risk_Management_Handbook.pdf

Riskikompassi. (3.3.2016)

http://riskikompassi.fi/johtaminen-riskienhallinta/viitekehyksia

Suortti JP., Salmijärvi S., Kupiainen J. 2015. Asioiden internet - Säästöä, kasvua vai molempia? (12.3.2016)

http://dif.fi/wp-content/uploads/boardview-lehti/2015/03/bv-1-2015-asioiden-internet-saastoa-kasvua-vai-molempia.pdf

Standars Australia/ Standars New Zealand 2004. Risk management guidelines (AZ/NZS 4360:2004) (3.3.2016)

file:///C:/Users/Tia/Downloads/Risk%20Management%20Guidelines%20Companion%20to%20AS%20NZS%204360%202004.pdf

The Institute of risk management: Cyber risk executive summary 2014 (2.3.2016)

https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf

Tietosuojavaltuutetun toimisto (20.4.2016)

http://tietosuoja.fi/fi/index/euntietosuojauudistus.html

Henkilölähteet:

Haastateltava A (Haastattelu 2.8.2016)

Haastateltava B (Haastattelu 20.12.2016)

Haastateltava C (Haastattelu 13.12.2016)

Haastateltava D (Haastattelu 14.12.2016)

Haastateltava E (Haastattelu 2.1.2017)

Haastateltava F (Haastattelu 3.1.2017)

LIITE 1: TEEMAHAASTATTELURUNKO VAKUUTUSYHTIÖILLE

HAASTATELTAVAN TAUSTATIEDOT

Kertoisitteko ensin koulutustaustastanne, työkokemuksestanne, asemastanne organisaatiossa sekä kyberturvallisuus osaamisestanne?

KYBERRISKIT

1. Kyberriskien asema Suomessa. Kuinka hyvin on tiedostettu riskit sekä kasvava uhka?
2. Mitkä ovat merkittävimmät kyberriskit joita vakuutetaan?
3. Millaisia uusia kyberriskejä syntyy tulevaisuudessa 1-5 vuoden sisällä?
4. Kyberriskeiltä suojautumisen tulevaisuus vakuutuksilla ja muilla riskienhallinnan keinoilla. Panostetaanko niiltä suojautumiseen enemmän?

KYBERVAKUUTUS

1. Millaiset yritykset ovat kybervakuutuksen kohderyhmää? (toimialat, koko)
2. Millainen on asiakkaiden tietoisuus kybervakuutuksesta ja sen ominaisuuksista?
3. Mitä palveluja kybervakuutuksen mukana tulee?
4. Yhteistyö IT- alan organisaatioiden kanssa? Millaisia etuja/haittoja?

KYBERVAKUUTUSMARKKINAT SUOMESSA

1. Millainen osa Suomen vakuutusmarkkinoita kybervakuutus on?
2. Kilpailu kybervakuutusmarkkinoilla?
3. Kysynnän ongelmat: ylihinnoittelu?
4. Myyntiprosessi? -> kyberturvallisuus analyysi?
5. Haitallinen valikoituminen sekä moraalikato kybervakuutuksessa?
6. Jälleenvakuuttajien rooli kyberriskien jakamisessa?

Olisiko teillä esittää aiheesta muita huomioita, joita ei tullut ilmi haastattelun aikana tai materiaalia, josta olisi hyötyä tutkimuksessani?

LIITE 2: TEEMAHAASTATTELURUNKO YRITYKSILLE

HAASTATELTAVAN TAUSTATIEDOT

Kertoisitteko ensin koulutustaustastanne, työkokemuksestanne, asemastanne organisaatiossa sekä kyberturvallisuus osaamisestanne?

KYBERRISKIT

1. Millaisena riskinä kyberriskit nähdään ja millaisia vahinkoja kyberriskit voivat aiheuttaa teidän organisaatiolle?
2. Miten kyberriskeihin on varauduttu? Millaisia riskienhallinnan menetelmiä käytetään?
3. Onko kybervakuutus otettu/suunnitteilla ottaa? Jos ei ole otettu, niin mitkä ovat syyt siihen?
4. Kuinka merkittävänä kyberuhkia pidetään muihin uhkiin nähden?
5. Tuleeko kyberriskien merkitys organisaatiollenne kasvamaan tulevaisuudessa? Aiheuttaako se muutoksia toimintatapoihinne?
6. Kyberriskien asema Suomessa. Kuinka hyvin on tiedostettu riskit sekä kasvava uhka?
7. Mitkä ovat merkittävimmät kyberriskit joita vakuutetaan?
8. Millaisia uusia kyberriskejä syntyy tulevaisuudessa 1-5 vuoden sisällä?
9. Kyberriskeiltä suojautumisen tulevaisuus vakuutuksilla ja muilla riskienhallinnan keinoilla. Panostetaanko niiltä suojautumiseen enemmän?

Olisiko teillä esittää aiheesta muita huomioita, joita ei tullut ilmi haastattelun aikana tai materiaalia, josta olisi hyötyä tutkimuksessani?